ProxyServer
Internet Access / Firewall

Dual Ethernet ProxyServer

Model MTPSR1-120

User Guide

MultiTech® Systems

User Guide

88301501 Revision B

Dual Ethernet ProxyServer (Model No MTPSR1-120)

This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved.

Copyright © 1999, by Multi-Tech Systems, Inc.

Multi-Tech Systems, Inc. makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Record of Revisions

Revision	Description
A (9/4/98)	Manual released. All pages at revision A.
B (2/19/99)	Manual revised for software version 2.00. All pages at revision B.

Patents

This Product is covered by one or more of the following U.S. Patent Numbers: ***5.301.274; 5.309.562***; ***5.355.365; 5.355.653; 5.452.289; 5.453.986***. Other Patents Pending.

TRADEMARK

Trademark of Multi-Tech Systems, Inc. is the Multi-Tech logo.
Windows is a registered trademark of Microsoft.

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(612) 785-3500 or (800) 328-9717
Fax 612-785-9874
Tech Support (800) 972-2439
Internet Address: http://www.multitech.com
Fax-Back (612) 717-5888

Contents

Chapter 1 - Introduction and Description

Introduction 6
Preview of this Guide 6
Front Panel Description 8
Back Panel Description 9
- RS232/V.35 Connector 9
- Ethernet 1 and 2 10Base-T Connectors 9
- Command Connector 9
- Power Connector 9

Specifications 10
- Ethernet Ports 10
- Command Port 10
- WAN Link 10
- Electrical/Physical 10

Chapter 2 - Installation

Safety Warnings 12
Unpacking Your Firewall 12
V.35 Shunt Procedure 13
Cabling Your Firewall 14

Chapter 3 - Software Loading and Configuration

Loading Your Software 18
Wizard Setup 20
- IP Wizard Setup 20
- Default WAN Link Configuration 22

Chapter 4 - Firewall Software

Introduction 26
Typical Applications 26
- Configuration 1 - Cable/DSL Modem 26
- Configuration 2 - Existing Dual-LAN with Router 27
- Configuration 3 - New Dual-LAN with T1 DSU 28

Firewall Program Group 30
Firewall Configuration 32
Changing IP Parameters 33
Changing WAN Port Parameters 35
Enabling PPP/SLIP 36
Enabling the DHCP Server 38
Adding Proxy Applications 39
- Filtering 40

Enabling Virtual Servers 41
Statistics 42
Applications 42

Chapter 5 - Remote Configuration and Management

Introduction 44
Remote Configuration 44
Modem-Based 44
LAN-Based 46
Remote Management 48
Telnet 48
WEB Management 50

Chapter 6 - Warranty, Service and Tech Support

Introduction 52
Limited Warranty 52
On-line Warranty Registration 52
Tech Support 53
Recording ProxyServer Information 53
Service 54
The Multi-Tech BBS 55
To Log on to the Multi-Tech BBS 55
To Download a File 55
About the Internet 56
About the Multi-Tech Fax-Back Service 56

Appendixes

Appendix A - TCP/IP (Transmission Control Protocol/Internet Protocol) Description 58
Appendix B - Cabling Diagrams 61
Appendix C - Regulatory Information 63

Glossary

Index

ProxyServer
Internet Access / Firewall

Chapter 1 - Introduction and Description

MultiTech® Systems

Introduction

Welcome to Multi-Tech's Dual Ethernet ProxyServer, model number MTPSR1-120 (hereafter, Firewall) a high speed Internet access device that provides firewall protection to your corporate secured (private) LAN and allows Internet access to the Internet Services Network (public LAN) that resides outside the firewall. Internet access can be provided through new technologies, such as cable or DSL modems, connecting to an existing high speed public LAN, or connecting the RS232 WAN port on the back of the unit that allows Internet access up to T1/E1 access speeds. The Firewall provides two Ethernet connections that implement firewall protection and gateway security for your LAN resources and provides megabit data transfer rates (up to 20 times faster than a 56K modem) for your Internet access.

The Firewall provides two Ethernet 10Base-T ports which connect your private secured LAN to the LAN 1 connection and the Internet Services Network resources to the LAN 2 connection, and a Command port for configuration. An additional RS232/V.35 port is provided for an alternate connection to an external WAN for connecting your secure corporate LAN directly to an ISP. System management is provided through the command port using bundled Windows® software which provides easy-to-use configuration menus.

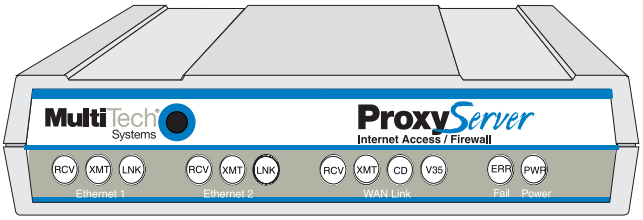


Figure 1-1. Firewall (MTPSR1-120)

Preview of this Guide

This guide describes the Firewall and tells you how to install and configure the unit. The information contained in each chapter is as follows:

Chapter 1 - Introduction and Description

Chapter 1 describes the Firewall's front panel indicators, and back panel connectors. In addition, a list of relevant specifications is provided at the end of the chapter.

Chapter 2 - Installation

Chapter 2 provides information on unpacking and cabling your Firewall. The installation procedure describes each cable connection. This chapter mirrors the procedures provided in your printed Firewall Quick Start Guide (PN 8207810x).

Chapter 3 - Software Loading and Configuration

Chapter 3 provides instructions for software loading and initial configuration. The Firewall software diskettes are Windows® based. Later chapters, as well as the included online Help, will describe the Firewall software in more detail.

Chapter 4 - Firewall Software

Chapter 4 describes the Firewall software package designed for the Windows ® environment. This chapter describes the Firewall software from an applications standpoint, and in so doing, not every screen is shown, nor is each field within a screen defined. For explanations and parameters of each field within a dialog box please refer to the online Help provided within the software.

Chapter 5 - Remote Configuration and Management

Chapter 5 provides procedures for changing the configuration of a remote Firewall. Remote configuration allows you to change the configuration of a unit by simply connecting two modems between the two Firewalls and remotely controlling the unit. In addition, remote management utilities such as Telnet and Web-based management of the Firewall.

Chapter 6 - Warranty, Service and Tech Support

Chapter 6 provides instructions on getting service for your Firewall at the factory, a statement of the limited warranty, information about our Internet presence, and space for recording information about your Firewall prior to calling Multi-Tech's Technical Support.

Appendixes

Appendix A - TCP/IP (Transmission Control Protocol/Internet Protocol) Description

Appendix B - Cabling Diagrams

Appendix C - Regulatory Information

Front Panel Description

The front panel, shown in Figure 1-2, contains four groups of LEDs that provide the status of the LAN connection, link activity, and general status of the Firewall. The Ethernet 1 and Ethernet 2 LEDs display the activity of the public and private LANs, in whether the Firewall is connected to the LAN, transmitting or receiving packets, and if a collision is in progress. The WAN Link LEDs display the status of the RS232/V.35 WAN link, that can optionally be connected to an external Data Communications Equipment (DCE) device, in whether the link is ready to transmit or receive serial data, and if an external communications device with a V.35 interface is connected to the Firewall. The last group of LEDs indicate whether the self test passed or failed and if the power On/Off switch on the back of the Firewall is turned On.

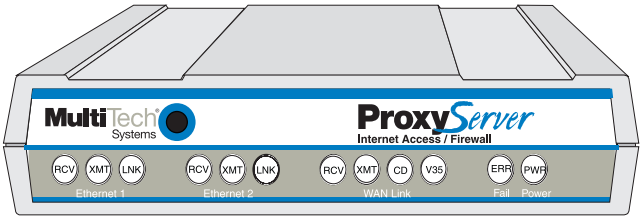


Figure 1-2. Front Panel

ETHERNET 1 and 2

RCV Receive Data indicator blinks when packets are being received from the private (Ethernet 1) or public (Ethernet 2) LANs.

XMT Transmit Data indicator blinks when packets are being transmitted to the private (Ethernet 1) or public (Ethernet 2) LANs.

LNK Link indicator lights when the Ethernet link senses voltage from a concentrator or external device.

WAN Link

RCV Receive Data indicator blinks when packets are being sent to the local area network.

XMT Transmit Data indicator blinks when packets are being transmitted from the local area network.

CD Carrier Detect indicator lights when a carrier signal is detected on the WAN link.

V35 V.35 indicator lights when internal shunt is set for V.35 operation.

Fail

ERR Error indicator lights when the Firewall is booting or downloading setup.

Power

PWR Power indicator lights when power is applied to the Firewall.

Back Panel Description

The cable connections for the Firewall are made at the back panel. In addition to the Power connector, Three groups of connectors are used on the Firewall: the Command Port, Ethernet 1 & 2 (10BASET) and RS232/V.35. The cable connections are shown in Figure 1-3 and defined in the following groups.

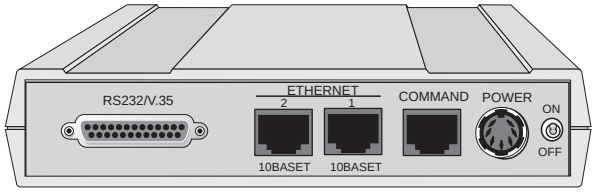


Figure 1-3. Back Panel

RS232/V.35 Connector

The RS232/V.35 (DB-25) connector is used to connect the Firewall to an external modem, DSU, or other Data Communications Equipment (DCE). This connection can be either RS232C (default) or V.35. If the connection is V.35, then the shunt must be moved from the default RS232 position to the V.35 position (for details on this procedure, refer to Chapter 2 - V.35 Shunt Procedure).

Ethernet 1 and 2 10Base-T Connectors

The Ethernet 10Base-T connectors are used to connect the Firewall to a LAN using unshielded twisted cable. Ethernet 1 connects the Secured (private) LAN, and Ethernet 2 connects the Internet (public) LAN. These connectors are RJ-45 jacks.

Command Connector

The Command connector is used to configure the Firewall using a PC with a serial port and running Windows® software. The Command connector is an RJ-45 jack and a short adapter cable is provided to convert to a standard serial port DB-25 female connector.

Power Connector

The Power connector is used to connect the external power supply to the Firewall. The Power connector is a 6-pin circular DIN connector. A separate power cord is connected to the power supply and the live AC grounded outlet.

Specifications

- Protocols - Point-To-Point Protocol (PPP), and Serial Line Internet Protocol (SLIP)

Ethernet Ports

- Two Ethernet Interface - 10Base-T (twisted pair) RJ-45 connectors.

Command Port

- Single 19.2K bps asynchronous Command Port using a short RJ-45 to DB-25 cable with a DB-25 female connector

WAN Link

- One RS232/V.35 port connector.

Electrical/Physical

- Voltage - 115 VAC (Standard), 240 Volts AC (Optional)
- Frequency - 47 to 63 Hz
- Power Consumption - 10 Watts
- Dimensions - 1.625" high x 6" wide x 9" deep

  5.63cm high x 22.34cm wide x 33.51cm deep
- Weight - 2 pounds (.92 kg)

ProxyServer
Internet Access / Firewall

Chapter 2 - Installation

MultiTech® Systems

Safety Warnings

1. Never install telephone wiring during a lightning storm.
2. Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
3. Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
4. Use caution when installing or modifying telephone lines.
5. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electrical shock from lightning.
6. Do not use the telephone to report a gas leak in the vicinity of the leak.

Unpacking Your Firewall

The shipping box contains the Firewall, external power supply, power cord, Command Port (DB-25 to RJ-45) cable, your Quick Start Guide, and three diskettes (i.e., this Firewall User Guide, and the Firewall Software). Inspect the contents for signs of any shipping damage. If damage is observed, do not power up the unit, contact Multi-Tech's Technical Support for advice (refer to Chapter 6). If no damage is observed, place the Firewall in its final location and continue with the next section.

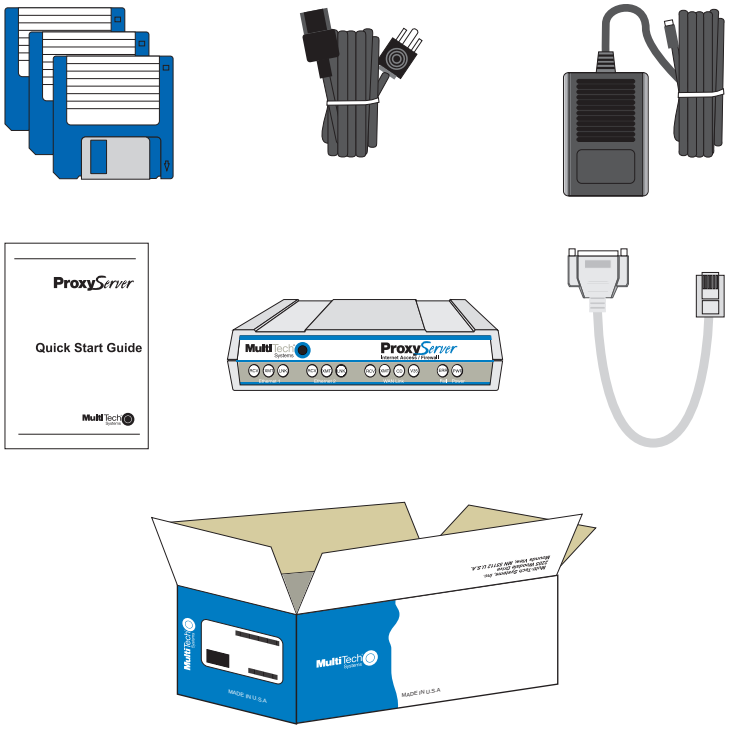


Figure 2-1. Unpacking

V.35 Shunt Procedure

If you are using an external DCE device on the WAN RS232/V.35 port, and the connection will be a V.35 connection, the internal shunt must be moved from the RS232C (default) position prior to cabling and power-up. The following steps detail the procedures for switching the shunt.

Step	Procedure
1	Ensure that the external power supply is disconnected from the Firewall.
2	Turn the Firewall over and remove the cabinet mounting screw from the chassis.

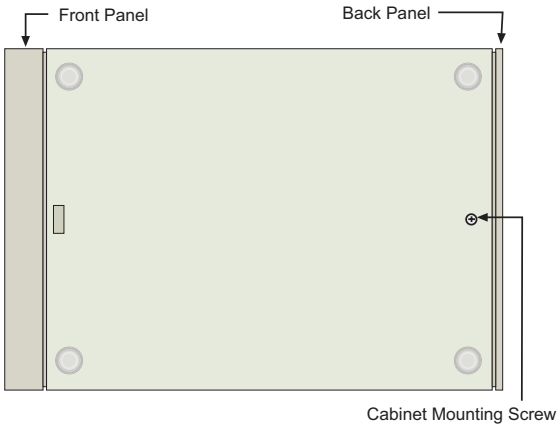


Figure 2-2. Cabinet Mounting Screw

3	Being sure to support the back panel, turn the Firewall right-side-up, tilt the back panel down, and slide the circuit board out of the chassis.
4	Place the unit on a flat, grounded surface with the LED's facing you.
5	Gently pry the shunt out of the RS232 position, and insert it in the V.35 position.

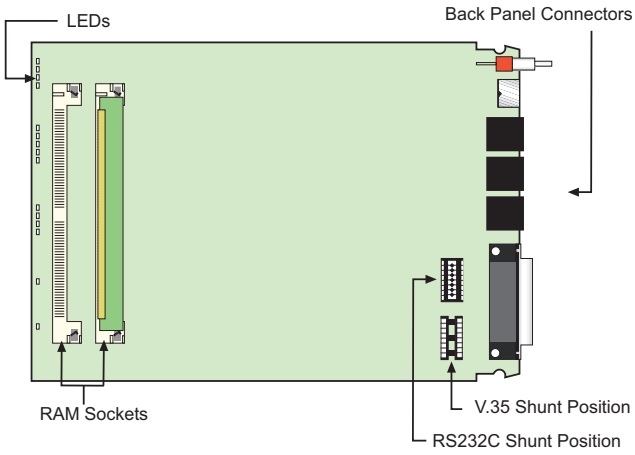


Figure 2-3. Shunt Positions

6	Align the board with the guide slots on the inside of the chassis and carefully slide the board back into the chassis.
7	Being sure to support the back panel, turn the Firewall over again, and replace the cabinet mounting screw.
8	Turn the Firewall right-side-up again and proceed to the next section to connect the cables.

Cabling Your Firewall

Cabling your Firewall involves making the proper Power, Command Port, and Ethernet connections. An optional WAN connection is provided to connect to an external WAN device. Figure 2-4 shows the back panel connectors and the associated cable connections, and the table that follows details the procedures for connecting the cables to your Firewall.

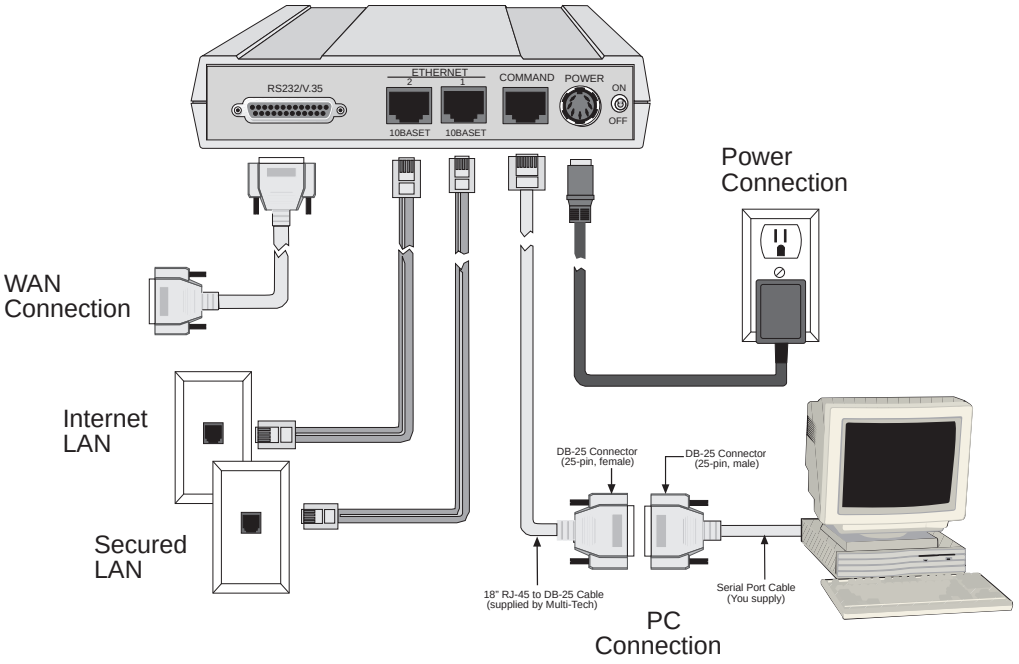


Figure 2-4. Cable Connections

Cabling Procedure

Step	Procedure
1.	Connect one end of the power supply to a live AC outlet and connect the other end to the Firewall as shown in Figure 2-4. The power connector is a 6-pin circular DIN connector.
2.	Connect the Firewall to a PC by using the short RJ-45 to DB-25 (female) cable provided in your unit. Plug the RJ-45 end of the cable into the Command port of the Firewall and the other end into the RS-232 cable (you supply) from the PC serial port. See Figure 2-4.
3.	To connect your secure (private) LAN, connect one end of an RJ-45 (UTP) cable to the LAN 1 connector on the back of the Firewall. Connect the other end of the cable to your private LAN.
4.	To connect a cable modem, DSL modem, or your Internet (public) LAN, connect one end of an RJ-45 (UTP) cable to the LAN 2 connector on the back of the Firewall. Proceed to step 6.
5.	If a cable modem, DSL modem, or your Internet LAN is being used, no cable connection will be made to the RS232/V.35 connector on the back of the Firewall. If the RS232/V.35 connector on the Firewall is going to be connected to a WAN device (i.e., connecting your secure (private) LAN to an ISP, connect one end of an RS232 or V.35 interface cable to the RS232/V.35 connector on the back of the Firewall. Connect the other end of this cable to the WAN device.

6. Turn on power to the Firewall by placing the ON/OFF switch on the back panel to the ON position. **Wait** for the Fail LED on the Firewall to go OFF before proceeding. This may take a couple of minutes to go OFF.

At this time your Firewall is completely cabled. Proceed to Chapter 3 to load the Firewall software.

ProxyServer
Internet Access / Firewall

Chapter 3 - Software Loading and Configuration

MultiTech® Systems

Loading Your Software

The following loading procedure does not provide every screen or option in the process of installing the Firewall software. The assumption is that the installation is being performed by a technical person with a thorough knowledge of Windows and the software loading process. Additional information on the Firewall software is provided in the Chapter 4, and in the on-line help provided with your Firewall software.

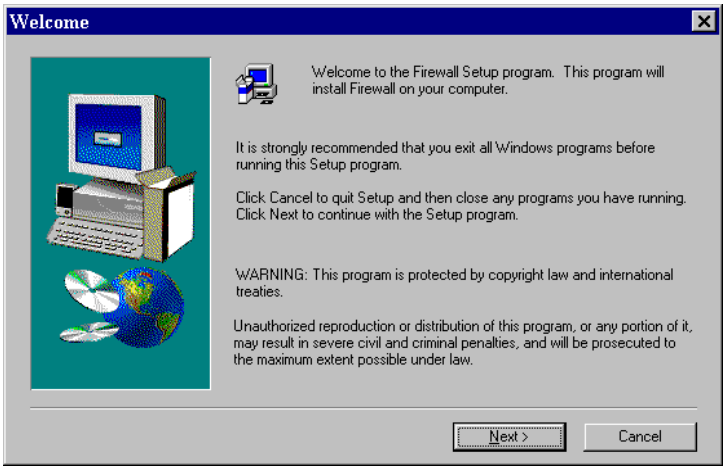
1. Run Windows on the PC connected to the Command Port.

2. Insert the Firewall disk labeled ***Disk 1*** into the disk drive on the PC connected to the Command port.

3. **Win3.1 users** - In Program Manager click **File | Run**. In the **Run** dialog box, type **a:\setup.exe** or **b:\setup.exe** (depending on the letter of your floppy disk drive) in the Command Line field and then click **OK**.

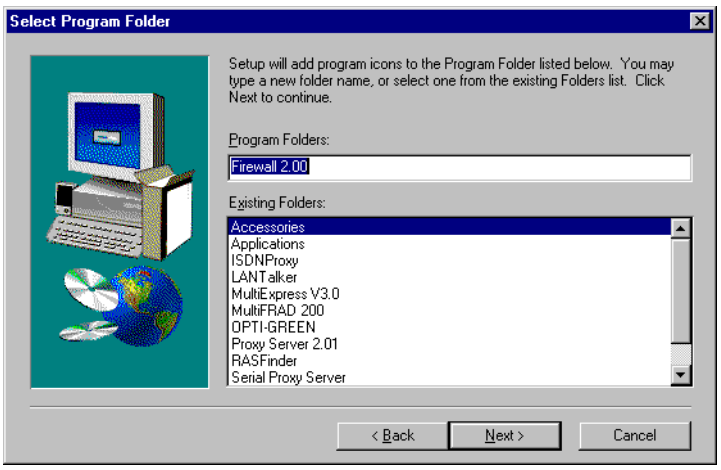
   Win95/NT users - click **Start | Run**. In the Run dialog box click on the down arrow and choose **a:\setup** or **b:\setup** (depending on the letter of your floppy disk drive) in the Command Line field and then click **OK**.

4. The Welcome screen is displayed.


Welcome
Welcome to the Firewall Setup program. This program will install Firewall on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Next >
Cancel

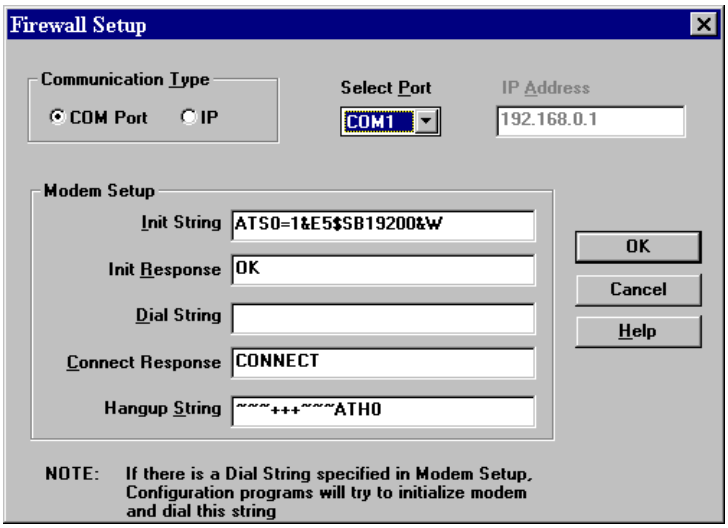
   Click **Next >** or press **Enter** to continue.

5. Follow the on-screen instructions to install your Firewall software.



The **Select Program Folder** dialog box enables you to use the default or select a different name for the new program group for the Firewall 2.00 software. After accepting the default or selecting a different folder name, press **Enter** or click **Next >** to continue.

6. The next dialog box enables you to designate the COM port of your PC that is connected to the Firewall. On the **Select Port** field, click the down arrow and choose the COM port of your PC (COM1 -- COM4) that is connected to the Firewall.



Click **OK** to continue.

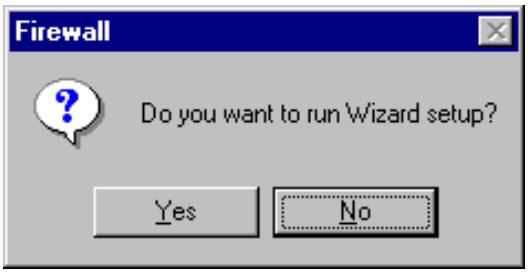
7. The **Setup Complete** dialog box is displayed.

Firewall Installed Successfully
Setup has finished installing Firewall on your computer.
Setup can launch the Read Me file and Firewall. Choose the options you want below.
Click Finish to complete Setup.
< Back
Finish

Click **Finish** to continue. The “Do you want to run Wizard setup?” message is displayed.

Wizard Setup

The Wizard Setup screen gives you a process for adding the basic information needed to configure your Firewall. This screen will guide you through entering the IP Address, Net Mask, and Default Route for your Secure (private) LAN. Then you can set up for static or dynamic addressing on the Internet LAN Port, set up the Gateway Parameters, and then do the same for the WAN port, if it is used.



9. Click **Yes** to run the Wizard Setup.

   Clicking **No** takes you to the program group (icons), where you can choose a utility from the program group.

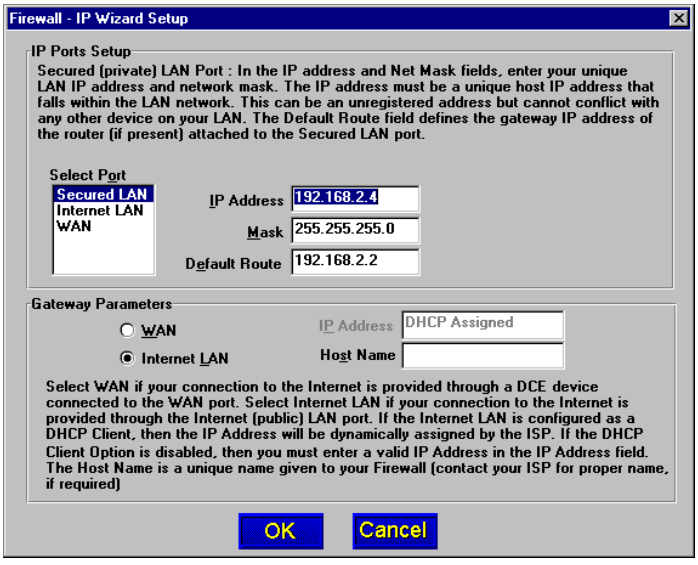
IP Wizard Setup

The IP Wizard Setup dialog box guides you through assigning LAN and WAN IP address information and determining if your LAN is already running a DHCP Server that will automatically assign Client IP addresses if enabled.

10. Change the default IP Address, Mask, and Default Route to the unique parameters for your Secure (private) LAN connected to the LAN 1 Port.

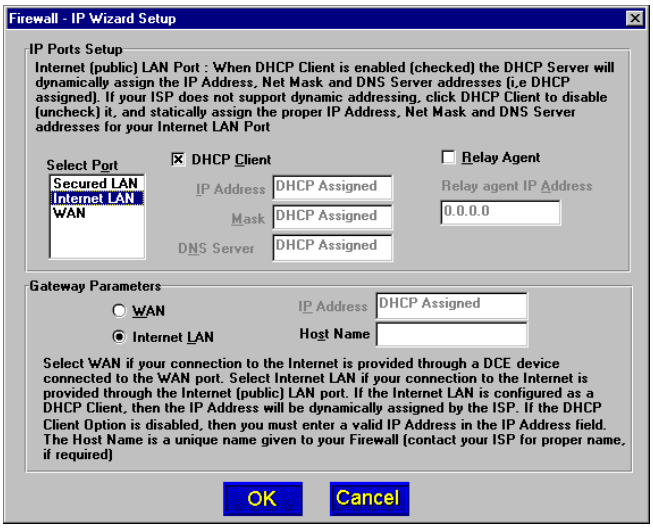
    Follow the on-screen instructions.

Secured LAN (LAN 1) Setup


Firewall - IP Wizard Setup
IP Ports Setup
Secured (private) LAN Port : In the IP address and Net Mask fields, enter your unique LAN IP address and network mask. The IP address must be a unique host IP address that falls within the LAN network. This can be an unregistered address but cannot conflict with any other device on your LAN. The Default Route field defines the gateway IP address of the router (if present) attached to the Secured LAN port.
Select Port
Secured LAN
Internet LAN
WAN
IP Address
192.168.2.4
Mask
255.255.255.0
Default Route
192.168.2.2
Gateway Parameters
WAN
Internet LAN
IP Address
DHCP Assigned
Host Name
Select WAN if your connection to the Internet is provided through a DCE device connected to the WAN port. Select Internet LAN if your connection to the Internet is provided through the Internet (public) LAN port. If the Internet LAN is configured as a DHCP Client, then the IP Address will be dynamically assigned by the ISP. If the DHCP Client Option is disabled, then you must enter a valid IP Address in the IP Address field. The Host Name is a unique name given to your Firewall (contact your ISP for proper name, if required)
OK
Cancel

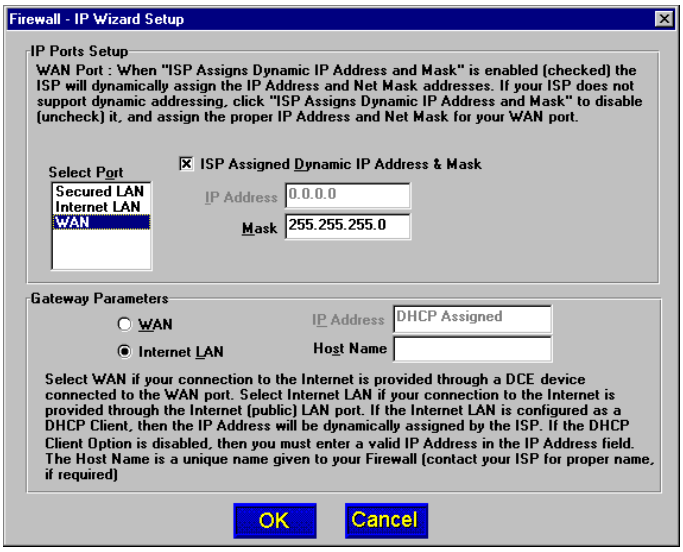
11. If an Internet (public) LAN is connected to the LAN 2 Port, click the **Internet LAN** option in the **Select Port** window, then either leave the **DHCP Client** option enabled or disable (uncheck) it and assign the proper IP Address, Net Mask, and DNS Server addresses for your Internet LAN. Follow the on-screen instructions and enter a Gateway IP Address, too, if the DHCP function is disabled.

Internet LAN (LAN 2) Setup


Firewall - IP Wizard Setup
IP Ports Setup
Internet (public) LAN Port : When DHCP Client is enabled (checked) the DHCP Server will dynamically assign the IP Address, Net Mask and DNS Server addresses (i.e DHCP assigned). If your ISP does not support dynamic addressing, click DHCP Client to disable (uncheck) it, and statically assign the proper IP Address, Net Mask and DNS Server addresses for your Internet LAN Port
Select Port
Secured LAN
Internet LAN
WAN
DHCP Client
IP Address
DHCP Assigned
Mask
DHCP Assigned
DNS Server
DHCP Assigned
Relay Agent
Relay agent IP Address
0.0.0.0
Gateway Parameters
WAN
Internet LAN
IP Address
DHCP Assigned
Host Name
Select WAN if your connection to the Internet is provided through a DCE device connected to the WAN port. Select Internet LAN if your connection to the Internet is provided through the Internet (public) LAN port. If the Internet LAN is configured as a DHCP Client, then the IP Address will be dynamically assigned by the ISP. If the DHCP Client Option is disabled, then you must enter a valid IP Address in the IP Address field. The Host Name is a unique name given to your Firewall (contact your ISP for proper name, if required)
OK
Cancel

WAN Setup

12. If a WAN device is connected to the WAN Port (marked **RS-232/V.35**), click the **WAN** option in the **Select Port** window, then either leave the **"ISP Assigned Dynamic IP Address & Mask"** option enabled or disable (uncheck) it and assign the proper IP Address and Net Mask for your WAN port. If your connection to the Internet is through the WAN port, follow the on-screen instructions: select WAN for the Gateway, then enter a Gateway IP Address and a Host Name in the fields provided.


Firewall - IP Wizard Setup
IP Ports Setup
WAN Port : When "ISP Assigns Dynamic IP Address and Mask" is enabled (checked) the ISP will dynamically assign the IP Address and Net Mask addresses. If your ISP does not support dynamic addressing, click "ISP Assigns Dynamic IP Address and Mask" to disable (uncheck) it, and assign the proper IP Address and Net Mask for your WAN port.
Select Port
Secured LAN
Internet LAN
WAN
ISP Assigned Dynamic IP Address & Mask
IP Address
0.0.0.0
Mask
255.255.255.0
Gateway Parameters
WAN
Internet LAN
IP Address
DHCP Assigned
Host Name
Select WAN if your connection to the Internet is provided through a DCE device connected to the WAN port. Select Internet LAN if your connection to the Internet is provided through the Internet (public) LAN port. If the Internet LAN is configured as a DHCP Client, then the IP Address will be dynamically assigned by the ISP. If the DHCP Client Option is disabled, then you must enter a valid IP Address in the IP Address field. The Host Name is a unique name given to your Firewall (contact your ISP for proper name, if required)
OK
Cancel

13. Click **OK** when you are finished configuring the IP parameters. The **Default WAN Link(s) Setup** dialog box is displayed.

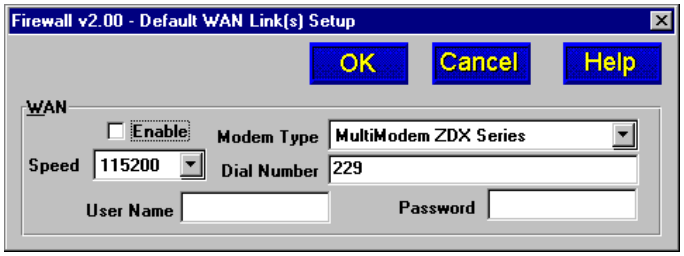
Default WAN Link Configuration

The **Default WAN Link(s) Setup** dialog box is used only if a device is connected to the RS-232/V.35 connector on the back panel of the Firewall. This connection enables your Secure (private) LAN to be connected to a local ISP for Internet service.

However, if you are using the **LAN 2** port, then you will have to *disable* the RS-232/V.35 WAN port on this dialog box.

14. If a cable modem, DSL modem, or Internet LAN is connected to LAN 2, click **OK** and proceed to step 19 to download the default setup.

    If a device is connected to the RS-232/V.35 connector on the back of the Firewall, proceed to step 15.



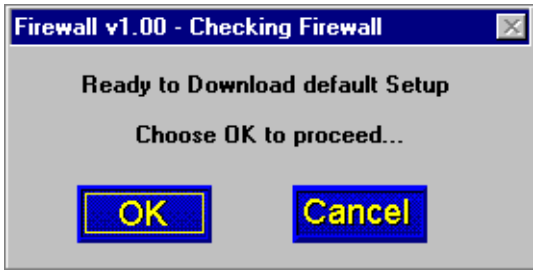
15. Click the down arrow for **Modem Type** and select from the listing the type of device that is connected to the RS-232/V.35 connector.

16. Click the **Dial Number** field and enter the phone number supplied by your ISP. The number can be a standard local number or it can include a long distance prefix.

17. Click the **User Name** field and enter the user name you negotiated with your ISP. The User Name can be up to 40 alphanumeric characters and is not case sensitive.

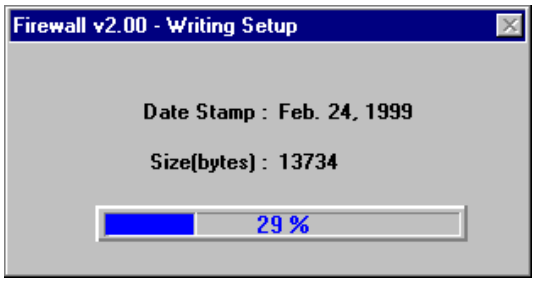
18. Click **Password** and enter the password you negotiated with your ISP. The password can be up to 15 alphanumeric characters and also is not case sensitive.

19. Turn on power to the Firewall and the following dialog box is displayed.



Click **OK** to proceed.

20. The **Writing Setup** dialog box is displayed as the setup configuration is written to the Firewall.



21. Check to ensure that the **Fail** LED on the Firewall is Off after the download is complete and the Firewall is rebooted.

22. **Win3.1 users** - you are returned to your Program Manager where the Firewall 2.00 Program Group and Program Items (Windows icons) have been created.

    Win95/NT users - you are returned to the Firewall 2.00 folder which will be open and visible on your desktop.

ProxyServer
Internet Access / Firewall

Chapter 4 - Firewall Software

MultiTech® Systems

Introduction

This chapter describes the software used in the Firewall. It begins with the description of three typical applications for the Firewall. These configuration examples are followed by a description of the Firewall program group, and examples of how to add some of the advanced features provided with the software.

Typical Applications

This section describes three typical applications for the Firewall. This is done with the assumption that the unit will be configured for a particular application during the initial installation. The three examples include a detailed diagram, along with a description of the process involved in setting up the configuration shown.

The first of the applications uses the Firewall to connect your Secured (private) LAN to the Internet using a cable or Digital Subscriber Line (DSL) modem, providing high speed Internet access. The second application ties your Secured (private) LAN and Internet (public) LAN through its router to the Internet. The third application is similar to the second, but uses a Data Communications Equipment (DCE) device—in this example, a T1 DSU—connected to the RS232 port on the back of the Firewall to connect to the Internet.

Configuration 1 - Cable/DSL Modem

In the configuration shown in Figure 4-1, the Firewall is connected to the Secured (private) LAN via the **LAN 1** connection of the back of the unit. Connection to the Internet is then provided by the cable or DSL modem by connecting the Ethernet connector on the modem to the **LAN 2** connection on the Firewall.

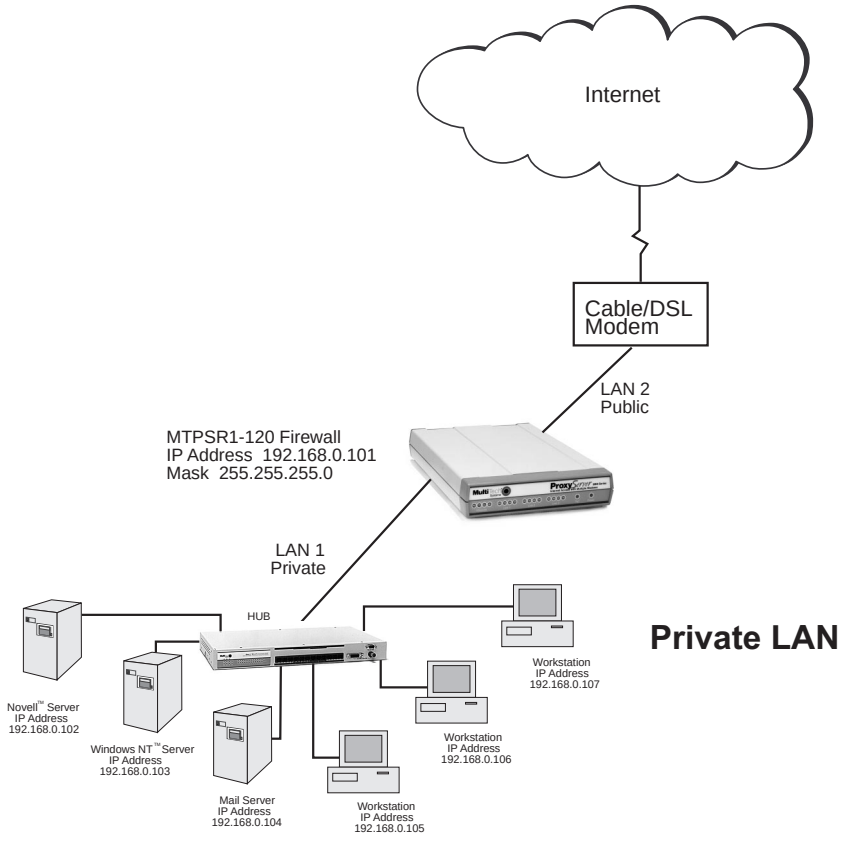
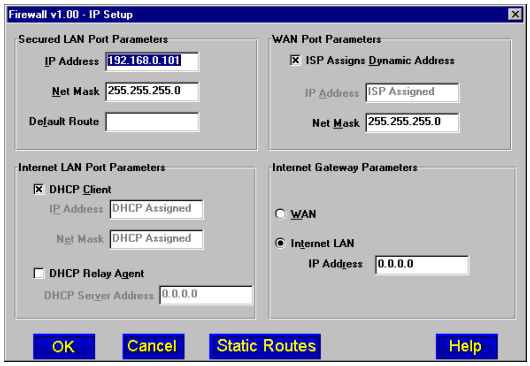


Figure 4-1. Cable/DSL Modem Configuration

During the loading of the Firewall software, the **Secured LAN Port Parameters** group (in the IP Setup dialog box) was configured to include an unregistered **IP Address** of 192.168.0.101 and default **Net Mask** of 255.255.255.0 for the Secured (private) LAN. The **Internet LAN Port Parameters** group was configured with the **DHCP Client** option active. This enables the Internet Services Provider (ISP) to dynamically provide the registered Internet IP addresses. If a static IP addressing scheme is provided by the ISP, then the DHCP Client field in the Internet LAN Port Parameters group is deactivated and the IP Address field becomes active. The static IP address is then entered in this field.



Configuration 2 - Existing Dual-LAN with Router

Another typical configuration ties the private LAN (LAN 1) to an existing Internet Services Network, which already provides Internet services. This configuration provides firewall and gateway security for the LAN users, and supports Internet access restrictions based on IP address, client protocols, or a list of forbidden sites.

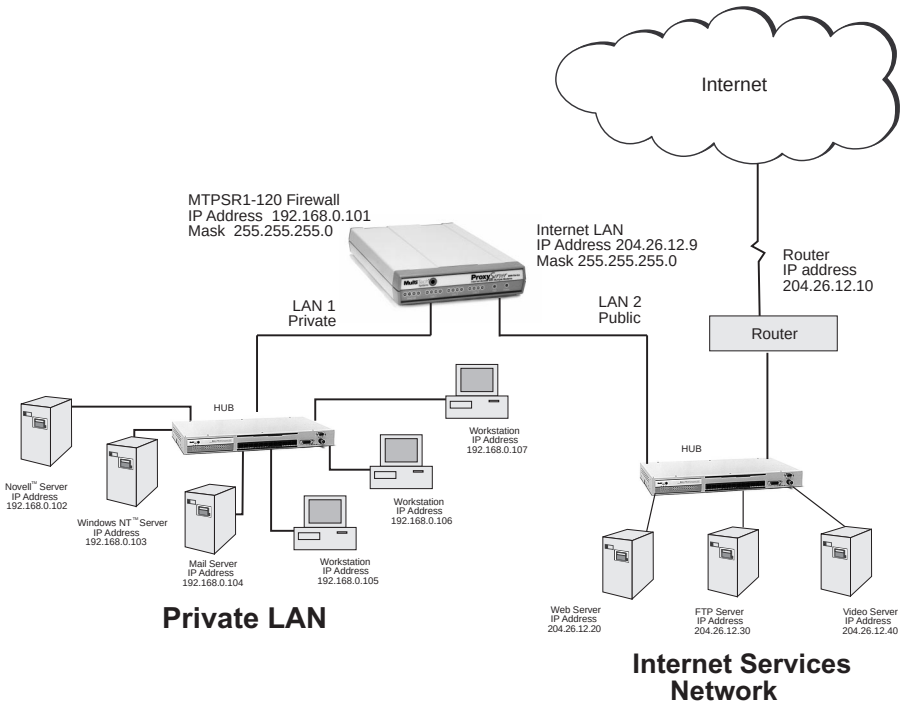
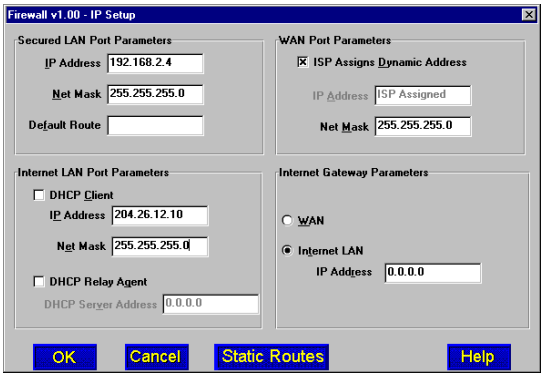


Figure 4-2. Existing Dual-LAN with Router Configuration

In the configuration shown in Figure 4-2, the Firewall is connected to the Secured (private) LAN via the **LAN 1** connection of the back of the unit. The Internet (public) LAN, is connected to the **LAN 2** connector on the back of the unit. Connection to the Internet is then provided by the existing router connected to the Internet Services Network.

During the loading of the Firewall software, the **Secured LAN Port Parameters** group (in the IP Setup dialog box) was configured to include an **IP Address** of 192.168.0.101, and a default **Net Mask** of 255.255.2.55.0 for the Secured (private) LAN. The **Internet LAN Port Parameters** group was configured with the **DHCP Client** option disabled, and the static **IP Address** of 204.26.12.10 was entered. This address is the existing static IP address that had already been assigned to the Internet Services Network router. A **Net Mask** of 255.255.255.0 was then entered to complete the configuration of the Internet (public) LAN.



Configuration 3 - New Dual-LAN with T1 DSU

The final typical configuration adds Internet services to existing LAN users. With this configuration, the Secured (private) LAN is secured by the firewall while the Internet Services Network is outside the firewall allowing Internet users to access the Internet (public) LAN resources, such as the Web, FTP, etc. servers. The Internet connection is provided with a T1 DSU connected to the RS232 connection on the back of the unit.

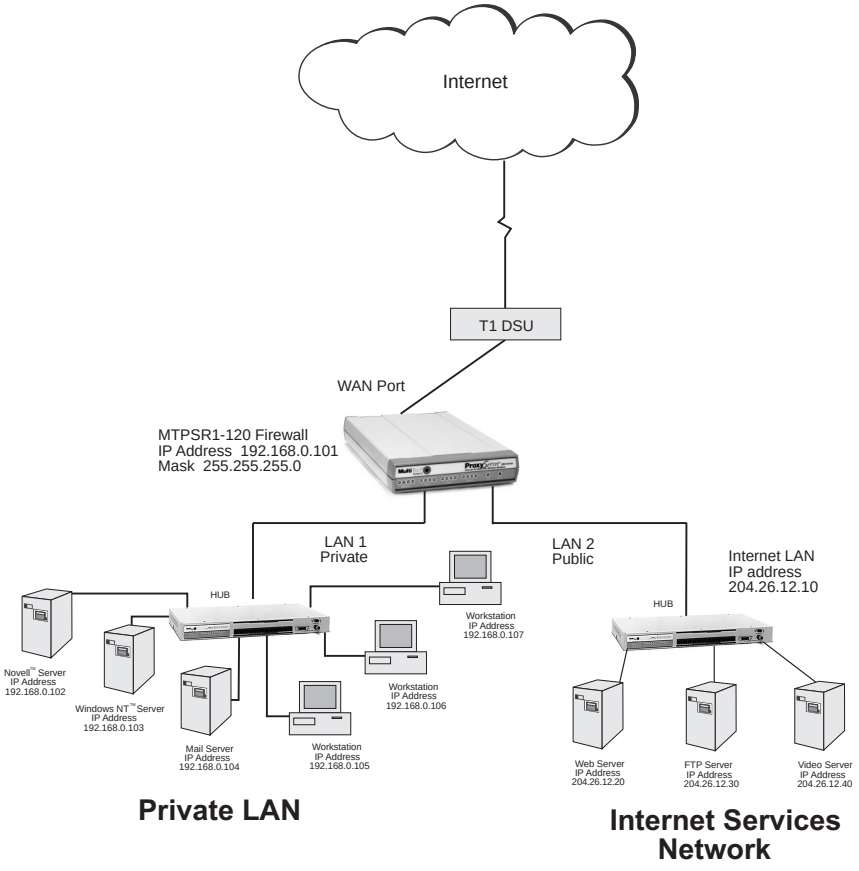
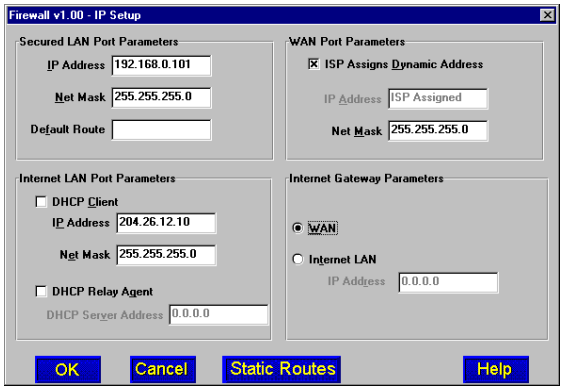


Figure 4-3. New Dual-LAN with T1 DSU Configuration

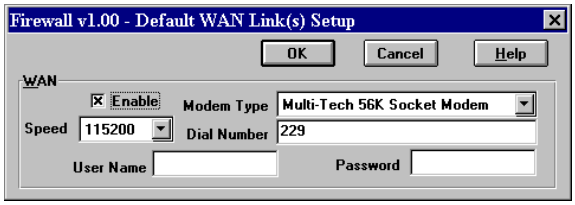
In the configuration shown in Figure 4-3, the Firewall is connected to the Secured (private) LAN via the **LAN 1** connection of the back of the unit. The Internet (public) LAN is connected to the **LAN 2** connector on the back of the unit. Connection to the Internet is then provided by a T1 DSU connected to the **RS232/V.35** connector on the back of the unit.

During the loading of the Firewall software, the **Secured LAN Port Parameters** group (in the IP Setup dialog box) was configured to include an unregistered **IP Address** of 192.168.0.101 and default **Net Mask** of 255.255.255.0 for the private LAN (LAN 1).



The **Internet LAN Port Parameters** group is either configured with the **DHCP Client** option active, enabling the ISP to dynamically provide the registered Internet IP addresses, or with the **DHCP Client** option disabled if a static IP addressing scheme is provided by the ISP. If the DHCP Client field is deactivated the static **IP Address** of 204.26.12.10 is then entered and the **WAN** option is checked in the **Internet Gateway Parameters** group.

In the **Default WAN Link Setup** dialog, the **WAN Enable** option is activated.



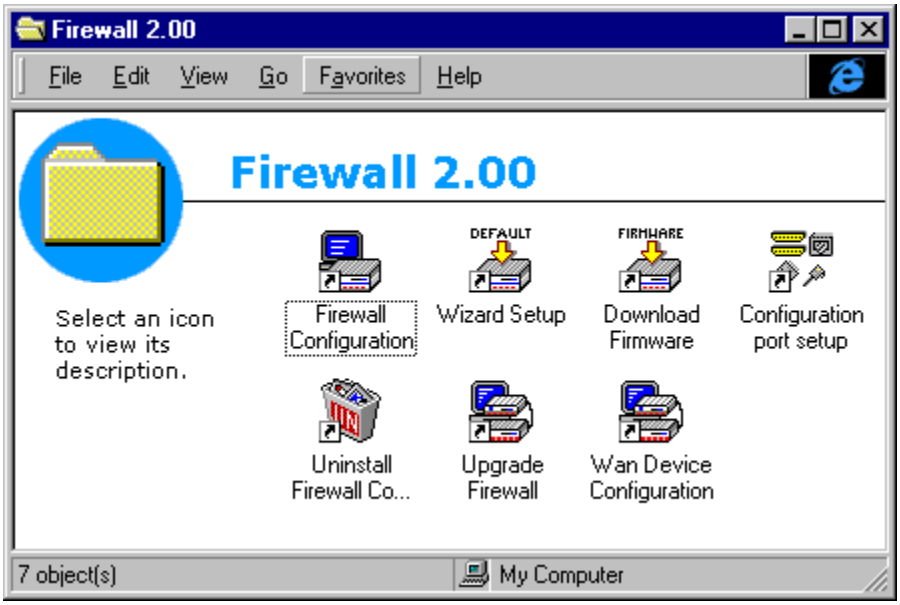
In the **Dial Number** field, the number for the ISP is entered and in the **User Name** and **Password** fields, the user name and password agreed upon with the ISP are entered.

The sections that follow provide examples of how to add some of the advanced features that enhance and build upon this basic setup.

Firewall Program Group

This section describes the advanced features of your Firewall software. The major configuration parameters are set when the software is loaded into your PC and the setup configuration is downloaded to the Firewall at the conclusion of the software installation. Our intent is not to cover every dialog box nor every field within a dialog box. The online Help provided with your software provides such definitions, along with explanations of parameters and defaults where applicable. This constitutes a dynamic help system in that the information presented always relates to the dialog box or window that is currently open.

Your Firewall Program Group contains several applications which provide the maximum flexibility for configuration and use. These applications are also accessible in Windows by clicking **Start | Programs | Firewall | *(application)***. The various options include Firewall Configuration, Wizard Setup, Download Firmware, Configuration Port Setup, Uninstall Firewall Configuration, Upgrade Firewall and Wan Device Configuration.



Firewall Configuration will be discussed in detail later in this chapter. A brief description of the other components is provided here:

Wizard Setup

This feature guides you through the download of the default settings to the Firewall. If you are installing for the first time, you can run Wizard Setup at the end of the installation before operating the Firewall. If you have made changes to the Firewall Configuration and wish to revert to the default setup, you can do so through the Firewall Program Group.

Choose **Wizard Setup** to download the factory default settings. If the Firewall is running, you will be queried to reboot. Click **Yes** to continue with the download. You will then be presented with two dialogs including **IP Setup** and **Default WAN Link(s) Setup**. These screens will contain the original setup information. Click **OK** on each to accept the default settings, or make any necessary changes and then click **OK**. When prompted, click **OK** again to proceed with the download. The default setup will be written to the Firewall. This process may take a few minutes. When it is finished, you will be returned to Windows.

Configuration Port Setup

The Configuration Port Setup program allows you to set up and configure the configuration port on your Firewall. This dialog is included in the initial installation process. Although parameters can be changed, be sure to note the current status of the software before making any alterations.

When you installed the Firewall software, you selected to configure the port as either an IP or COM Port. When COM Port is selected, you can assign the proper COM Port and define the modem Init String, Dial String, and various responses. If IP is selected, you can assign a static IP address or select one from the drop down list. For more information on each individual parameter, refer to the online Help provided with the software.

Download Firmware Update

This application allows you to update the firmware of the Firewall. This may be necessary in the case of repair or upgrade. To download the firmware update, choose **Download Firmware Update** from the **Firewall Program Group**, and the **Open** dialog box is displayed (if the Firewall is running, you will be queried to reboot to update firmware; click **OK** to proceed and the **Open** dialog will be displayed).

By default, the Firewall software will display the proper firmware from the Firewall folder. Double click on this file in the **File Name** list.

The Downloading Code dialog is displayed, which includes a status bar to monitor the download. When the download is complete the Firewall will reboot. This process will take several minutes. After rebooting, you will be returned to Windows.

Uninstall Firewall Configuration

Selecting Uninstall Firewall Configuration will allow you to completely remove all the components of the Firewall Program Group. Upon selecting this option your will be queried for confirmation. Click **Yes** to continue with the uninstall, or click **No** to abort.

Note: You will not be able to use the Firewall without Firewall Configuration. If you remove the components, you will need to reinstall the software. Refer to your *Firewall Quick Start Guide* for installation instructions.

Upgrade Firewall

The Upgrade Firewall utility allows you to upgrade your Firewall without losing the default settings. Use this utility to update the firmware and software of a pre-configured Firewall running older software. When you run Upgrade Firewall, from the Firewall program group, or from the Start menu, Firewall will reboot and your configuration settings will be checked. The necessary information will be updated, while the settings you have configured will be preserved. To perform a fresh installation, choose Download Firmware, and then run the Wizard Setup to configure the Firewall.

WAN Device Configuration

If you have an external WAN device connected to the WAN port of the Firewall, this application will open the Firewall Print Console, a terminal emulation program, that will allow configuration of the external device.

Firewall Configuration

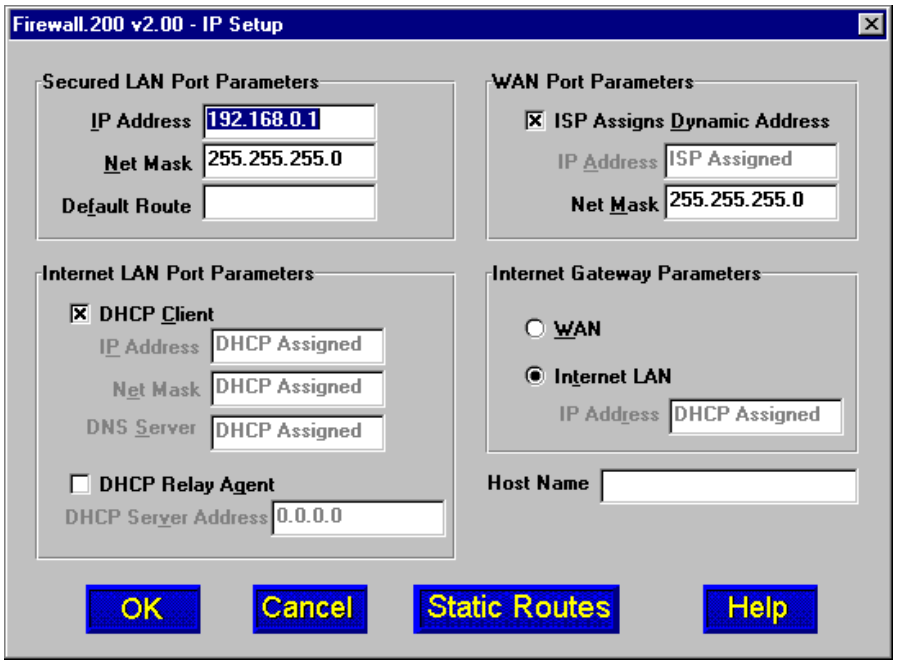
To view or change your Firewall configuration in Windows 95/98/NT, click on the **Start** | **Programs** | **Firewall** | **Firewall Configuration**. After loading, the **Firewall Setup** menu will appear.

The **Firewall Setup** menu consists of 13 buttons which allow you to display and change the protocol stacks, define the output of the Firewall, perform network management functions, test the communications link, print messages received from the target (the Firewall), and download setup information to the Firewall.

In the bottom row, there are two buttons to open the online Help system (Firewall Setup Help) and end (Exit) a Firewall configuration session.

Changing IP Parameters

The IP Setup dialog box establishes the IP addressing for your Secured (private) LAN, Internet (public) LAN, and, if the Firewall is directly connected to the Internet via the RS-232/V.35 connector, the WAN port. To change the IP Setup parameters that were configured during the Wizard Setup, click on the **IP** button in the **Firewall Setup** menu. The **IP Setup** dialog is displayed.



The **Secured LAN Port Parameters** group is used to assign the Ethernet parameters of your private LAN (LAN 1) port. If a router is used to connect a second private LAN, the IP address of that router is also entered in this group.

IP Address - This field defines the IP address of the private LAN (LAN 1) port on the ProxyServer. This must be a unique host IP address that falls in the LAN IP network, and can be an unregistered address.

Net Mask - This field defines the Subnetwork Mask of the private LAN (LAN 1) port on the Firewall.

Default Route - This field defines the IP address of a router on the private LAN that connects a second private LAN to the Firewall.

The **Internet LAN Port Parameters** group is used to configure the public LAN (LAN 2) port. The parameters of this group will vary, depending on the LAN configuration. The Internet LAN Port Parameters group defines the static or dynamic addressing scheme for the public LAN (LAN 2)

DHCP Client - If this option is active, the Internet Services Provider (ISP) is able to dynamically provide the registered Internet IP addresses. If a static IP addressing scheme is provided by the ISP, then the DHCP Client option must be deactivated and the IP Address field becomes active. The static IP address is then entered in this field.

IP Address - If the DHCP Client option is active, this address is dynamically assigned by the ISP. If the DHCP Client is inactive, then the static IP address of the router connected to the Internet Services Network is entered in this field.

Net Mask - If the DHCP Client option is active, the Net Mask is dynamically assigned by the ISP. If the DHCP Client is inactive, then the Net Mask of the router connected to the Internet Services Network is entered in this field.

DHCP Relay Agent - Enabling this option allows the Firewall to relay IP address requests from the Internet to the DHCP server through the WAN. If this option is enabled, the DHCP Server Address field becomes active, and the IP address of the DHCP server must be entered.

DHCP Server Address - If the DHCP Relay Agent option is active, enter the IP address of the DHCP server in this field.

The **WAN Port Parameters** group is used to configure the WAN port, if enabled. The WAN port parameters are established when the Firewall is directly connected to the Internet via the RS232/V.35 connector on the back of the unit.

ISP Assigns Dynamic Address - Normally, the ISP assigns a dynamic address when the port comes up. If this is not the case, disable this option and assign a valid registered Internet address in the IP Address field.

IP Address - If dynamic addressing is enabled, this field is dynamically assigned by the ISP. If static addressing is enabled, enter a valid Internet address in this field.

Net Mask - Enter the Subnetwork Mask for the WAN port in this field.

The **Internet Gateway Parameters** group is used to configure the Internet gateway if used by the Internet LAN (LAN 2) port.

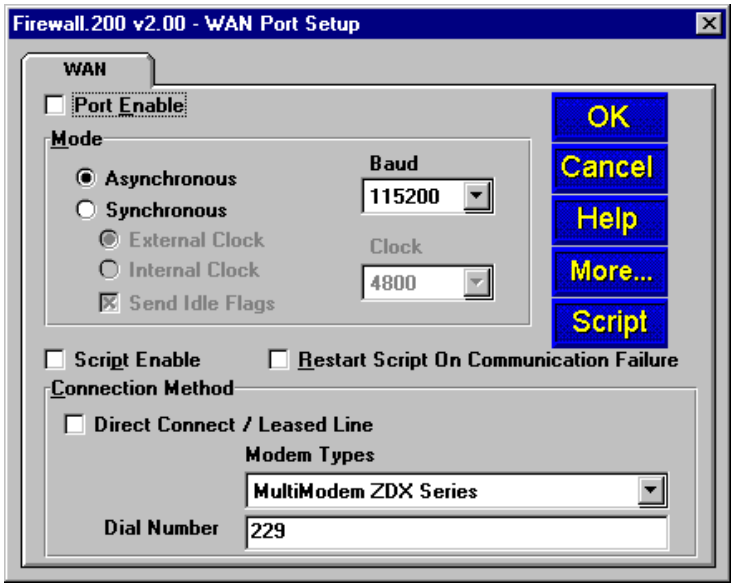
WAN - If a connection to the Internet Services Network is provided via a DCE device connected to the RS232/V.35 port on the back of the Firewall, then this option must be selected.

Internet LAN - If a connection to the Internet Services Network is provided through the Internet LAN (LAN 2), then this option must be selected. If the Internet LAN is configured as a DHCP Client, then the IP address will be dynamically assigned by the ISP. If the DHCP Client option is disabled, then a valid registered Internet address must be entered in the IP Address field.

IP Address - If the Internet LAN is configured as a DHCP Client, this address will be dynamically assigned by the ISP. If the DHCP Client option is disabled, the a valid registered Internet address must be entered in the IP Address field.

Changing WAN Port Parameters

In order to change the WAN port parameters of a DCE device connected to the RS232/V.35 connector on the Firewall, click on the **WAN** button in the **Firewall Setup** menu. The **WAN Port Setup** dialog box is displayed.



From this dialog, you can configure the parameters of the WAN port. To enable the WAN port, click on the **Port Enable** check box.

The **Mode** group allows you to configure the WAN interface to match the DCE device connected to the RS232/V.35 port on the Firewall. Options include **Asynchronous** or **Synchronous** mode. If asynchronous is chosen, you can select the proper **Baud** speed. If synchronous is chosen, **External Clocking** or **Internal Clocking** must be selected.

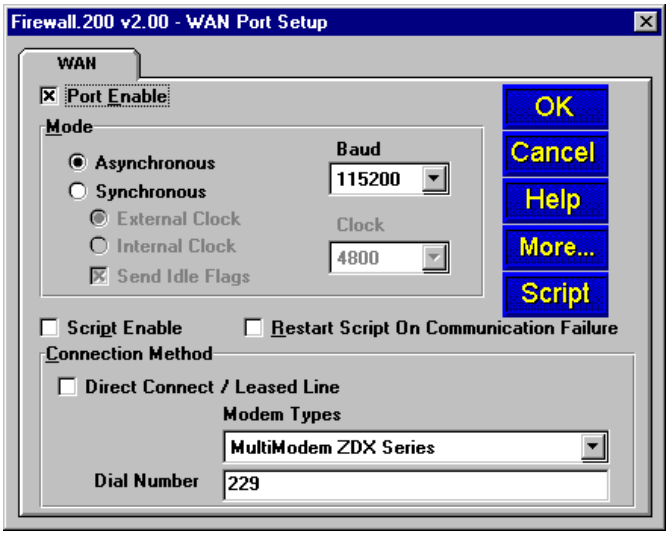
The **Connection Method** group allows you to configure the port as **Direct Connect/Leased Line**, and allows you to select the **Modem Type** and **Dial Number** for the DCE device.

For a detailed description of each field, refer to the online Help provided with your Firewall software.

Enabling PPP/SLIP

If you wish to use Point to Point Protocol (PPP) or Serial Line IP Protocol (SLIP) on the WAN port, you can enable it in the PPP/SLIP menu. In order to configure these options, you must first enable the WAN port.

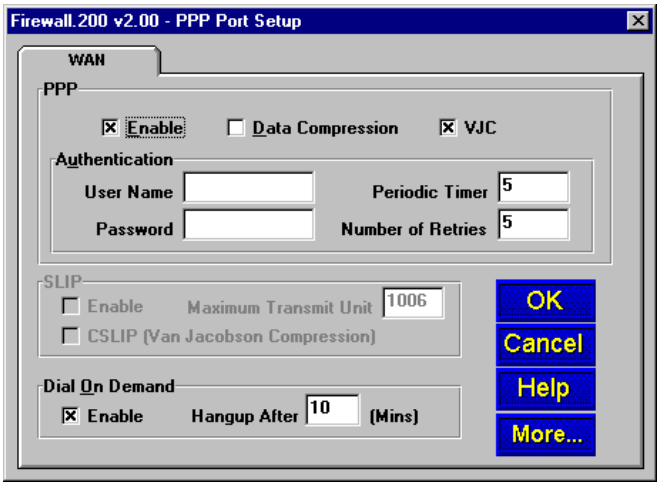
To enable the WAN port, click on the **WAN** button in the **Firewall Setup** menu. The **WAN Setup** dialog box appears.



Click on the **Port Enable** check box enable the WAN port. Click **OK**.

You are returned to the **Firewall Setup** menu. Click on **PPP/SLIP**. The **PPP Port Setup** menu is displayed.

Enabling PPP



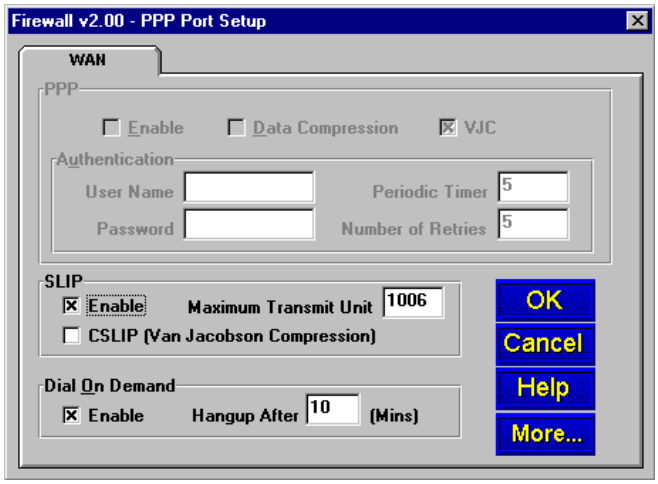
If you wish to configure the port for use with PPP, click on the **Enable** check box in the **PPP** group. Enter a valid **User Name** and **Password** and verify (or change) the **Periodic Timer** and **Number of Retries** (for definition and parameters of a specific field, refer to the online Help).

By default, Dial On Demand is enabled. If you do not wish to use this feature, click on the **Enable** check box in the **Dial On Demand** group to disable it.

When you have finished the configuration, click **OK**. You are returned to the **Firewall Setup** menu. Click **Download Setup** to save the new configuration to the Firewall.

Enabling SLIP

If you wish to configure the port for use with SLIP, click on the Enable check box in the SLIP group.



The following message appears:

Click **OK**. This value was assigned in the initial software installation and was downloaded to the ProxyServer at the end of the installation. If you wish to verify or change the WAN IP address, click on **IP** in the **Firewall Setup** menu.

If you wish to make use of CSLIP (Van Jacobsen Compression), click on the **CSLIP (Van Jacobsen Compression** check box to enable CSLIP. Verify (or change) the **Maximum Transmit Unit** value (for definition and parameters of a specific field, refer to the online Help).

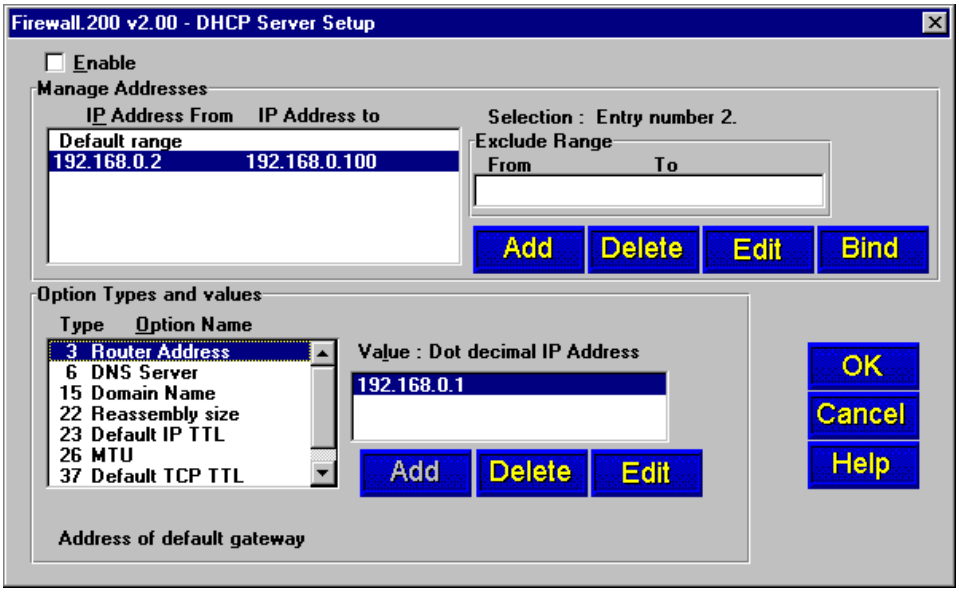
By default, Dial On Demand is enabled (checked). If you do not wish to use this feature, click on the **Enable** check box in the **Dial On Demand** group to disable (uncheck) it.

When you have finished the configuration, click **OK**. You are returned to the **Firewall Setup** menu. Click **Download Setup** to save the new configuration to the Firewall.

Enabling the DHCP Server

The DHCP Server feature of the Firewall manages all the IP address assignments on the Secured (private) LAN port. IP address management becomes completely transparent.

To enable the DHCP Server ability in the Firewall, click on the **DHCP Server** button in the **Firewall Setup** menu. The **DHCP Server Setup** dialog box appears.



The **DHCP Server Setup** menu allows you to customize each client PC configuration from one central point. You can establish a range of client addresses in the **Manage Addresses** group. You can then exclude specific addresses from that range in the **Exclude Range** field. You can also add, delete, edit and bind addresses using the corresponding buttons in this group.

The **Option Types and Values** group on the bottom portion of the menu allows you to customize the configuration of the client platform. Again, you can add, delete and edit an option by highlighting it and clicking on the appropriate button. You cannot, however, edit or delete entries provided in the default list.

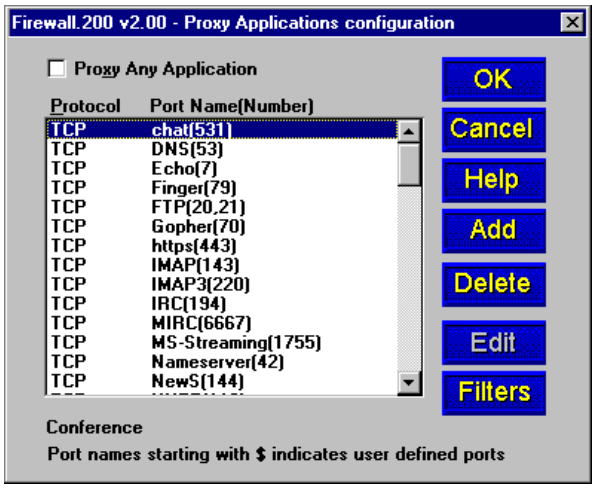
When you have finished the configuration, click **OK**. You are returned to the **Firewall Setup** menu. Click **Download Setup** to save the new configuration to the Firewall.

Adding Proxy Applications

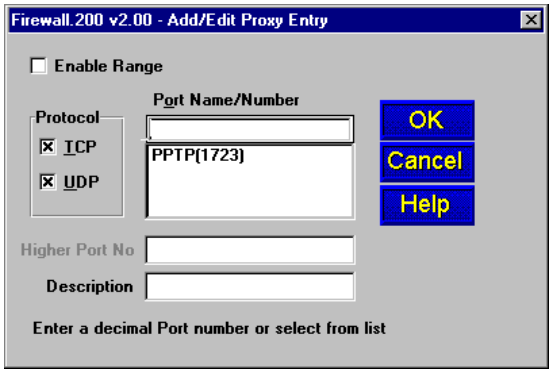
Certain software on your LAN may require a TCP or UDP port usage that is not currently supported by the Firewall. If this is the case, you must refer to the software documentation to determine the proper port usage and number. Without this information, the Firewall will not allow packets through to the Internet from the unknown software. Once the necessary information has been determined, you can add the application(s) to the supported list.

This list includes many of the most common port usages, however, not all are included because an increase in the number of port usages supported means a *possible* decrease in performance speed, and an increased security risk.

If you wish to add proxy applications that are not currently supported, click on the **Proxy Server** button in the **Firewall Setup** menu. The **Proxy Applications Configuration** dialog box appears. This menu includes a list of all the applications currently supported by the Firewall.



Click **Add**. The **Add/Edit Entry** dialog box appears.



This dialog will allow you to choose the desired protocol, and enter a **Port Name/Number** and **Description**. After you have entered these items, click **OK** to add the port usage to the list of supported usages.

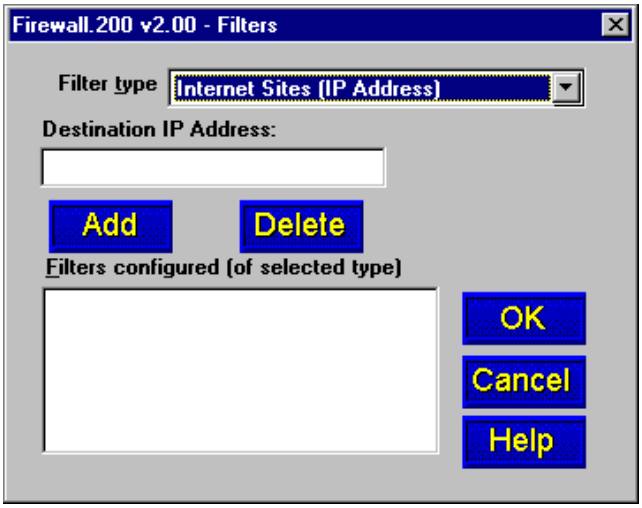
Filtering

The Filters dialog lets you configure the Firewall so that IP packets that are received by the server can be selectively filtered or forwarded based on their addresses or by the protocol ports to which they are destined.

The five filtering methods are:

- **Internet Sites (IP Address)** - In this method, IP packets can be filtered based on the IP address of an Internet Site. To add a new filter, enter the proper IP address in the **Destination IP Address** field and click **Add**.
- **Internet Sites (Domain Name)** - In this method, IP packets can be filtered based on the domain name of an Internet Site. To add a new filter, enter the proper domain name in the **Domain Name** field and click **Add**.
- **Client Workstations (IP Address)** - In this method, IP packets can be filtered based on the IP address of a Client workstation. To add a new filter, enter the workstation IP address in the **Source IP Address** field and click **Add**.
- **Client Workstations (MAC Address)** - In this method, IP packets can be filtered based on the MAC address of a Client workstation. To add a new filter, enter the workstation MAC address in the **MAC Address** field and click **Add**.
- **Applications** - In this method, IP packets can be filtered based on their specific purposes; e.g. Telnet packets (TCP based) or TFTP (UDP based) can be filtered or forwarded. To add a new filter, select the protocol from the **Protocol** drop down list, and select the application port from the **Port** drop down list, and click **Add**.

Filters that have been configured for each type will be displayed in the **Filters Configured (of selected type)** list, and can be deleted by selecting the filter entry and clicking **Delete**.



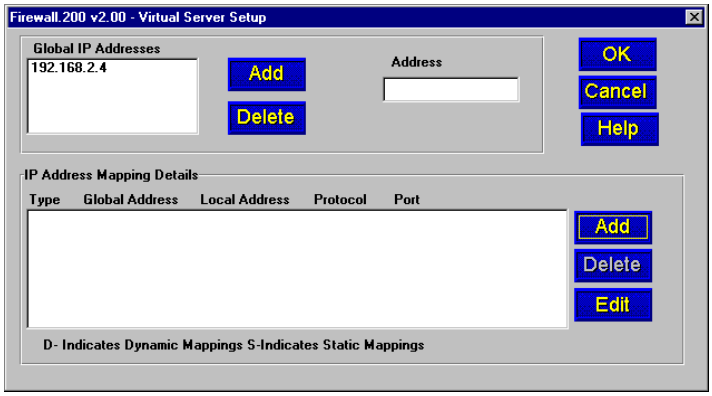
For a more detailed description of filtering, refer to the online Help provided with your Firewall software.

When you have finished adding applications, click **OK**. You are returned to the **Firewall Setup** menu. Click **Download Setup** to save the new configuration to the Firewall.

Enabling Virtual Servers

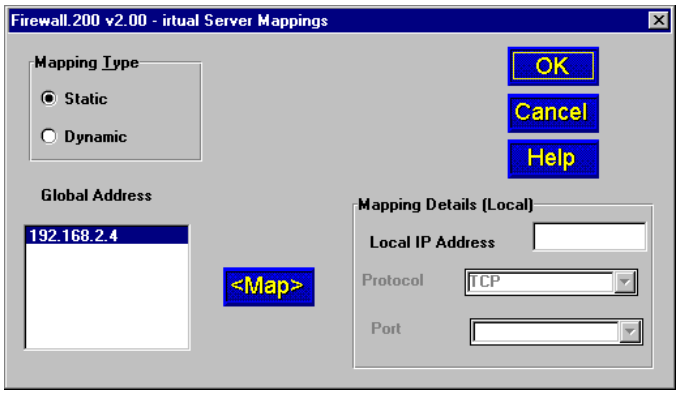
The Virtual Server Setup dialog box allows you to assign a virtual address to a statically assigned server. For example, if the ISP assigns static address of 200.2.9.1, you can set up a virtual server so that any requests sent to 200.2.9.1 will access 192.168.0.102.

Click on the **Virtual Servers** button in the **Firewall Setup** menu. The **Virtual Server Setup** dialog box appears.



To add a Virtual Server, type a valid IP address (200.2.9.1 in our example) in the **Address** field and then click **Add** in the **Global IP Addresses** group. The new address appears in the Global IP Addresses list.

Click **Add** in the **IP Address Mapping Details** group. The **Virtual Server Mappings** dialog box appears.



In the **Mapping Type** group, click on either **Static** or **Dynamic**. This will determine whether protocol and port usage will be entered statically, or assigned automatically by the server.

If the **Mapping Type** is **Static**, then enter the **Local IP Address** that the Global Address will be mapped to in the **Local IP Address** field, and click **Map**.

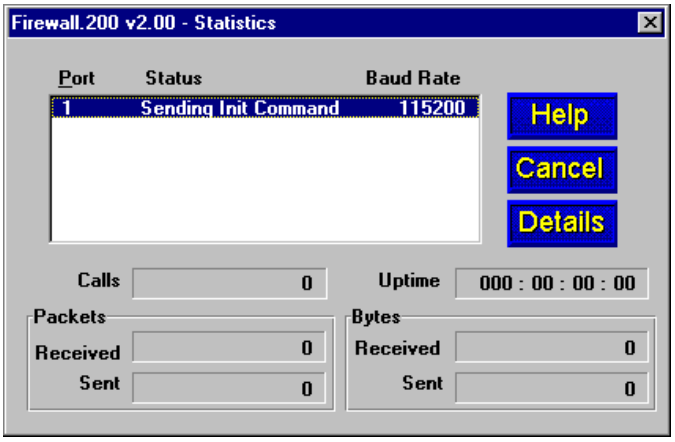
If the **Mapping Type** is **Dynamic**, then enter a **Local IP Address**, **Protocol** and **Port** in the appropriate fields and click **Map**.

The new mapping will be displayed in the **IP Address Mapping Details** group list.

When you have finished adding applications, click **OK**. You are returned to the **Firewall Setup** menu. Click **Download Setup** to save the new configuration to the Firewall.

Statistics

The Firewall is capable of providing statistics for the WAN port and for the whole system. These statistics can be useful for troubleshooting and management purposes. To access this information, click **Statistics** in the **Firewall Setup** menu. The **Statistics** dialog box is displayed.



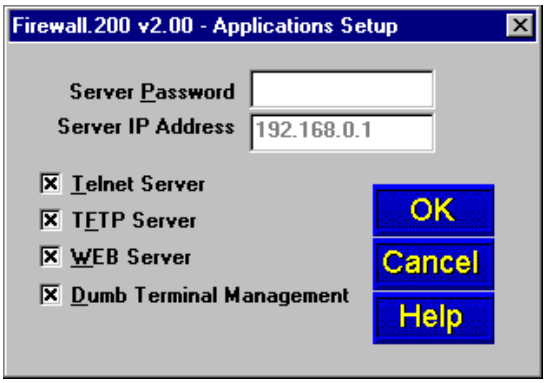
From this menu, you can query the details of the WAN port or observe total system statistics such as total system Uptime, and total Calls. In addition, statistics can be saved to a log file for future use.

For more details and parameters about specific fields within the statistics dialog, refer to the online Help.

Applications

In addition to local configuration, the Firewall supports various applications which allow it to be configured remotely from anywhere on the connected Internet. To manage these applications, click **Others** in the **Firewall Setup** menu.

The **Applications Setup** dialog box appears.



Enter a valid **Server Password** and **Server IP Address** (the IP address of the Firewall) and then verify that the desired applications are enabled. By default, the Firewall supports Telnet, TFTP, WEB, and Dumb Terminal management. If you wish to disable any of these applications, click the corresponding check box to disable (uncheck) support.

For more information on using these remote configuration applications, please refer to Chapter 5.

ProxyServer
Internet Access / Firewall

Chapter 5 - Remote Configuration and Management

MultiTech® Systems

Introduction

This chapter provides procedures for viewing or changing the configuration of a remote Firewall unit. Two methods are provided to access a remote unit; the first method is modem-based and the second method uses IP. Within the IP method, three applications can be used: 1) LAN-based using Trivial File Transfer Protocol (TFTP), 2) Telnet as a client application, and 3) a standard Web browser on the Internet.

Remote Configuration

Remote configuration requires that the Firewall software be loaded on the local PC. The local PC then controls the remote Firewall wiether via the modem connection, or via the LAN.

Modem-Based

To configure a remote Firewall, a local PC must have the Firewall software installed and configured to dial the remote Firewall, and must be connected to a dial-up line (i.e., modem). The remote Firewall needs to have a modem connected to both a dial-up line and the Command Port of the Firewall.

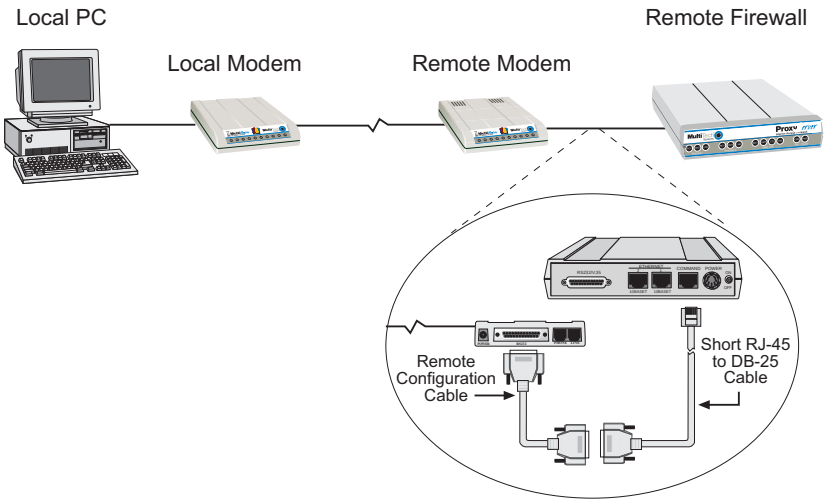


Figure 5-1. Modem-Based Remote Configuration

Once the connection to the remote unit is made, you can change the configuration as you see fit, and once changed, you can download the new configuration to the remote Firewall. The following procedure guides you through the setup of a modem-based remote configuration.

1 At the remote site, disconnect the the serial cable (attached to the PC) from the short RJ-45 to DB-25 cable attached to the Command Port of the Firewall.

2 Connect a Remote Configuration Cable (a serial cable with male connectors on both ends) to the short RJ-45 to DB-25 cable attached to the Command Port of the Firewall and to the RS-232 connector on the modem (see Figure 5-1).

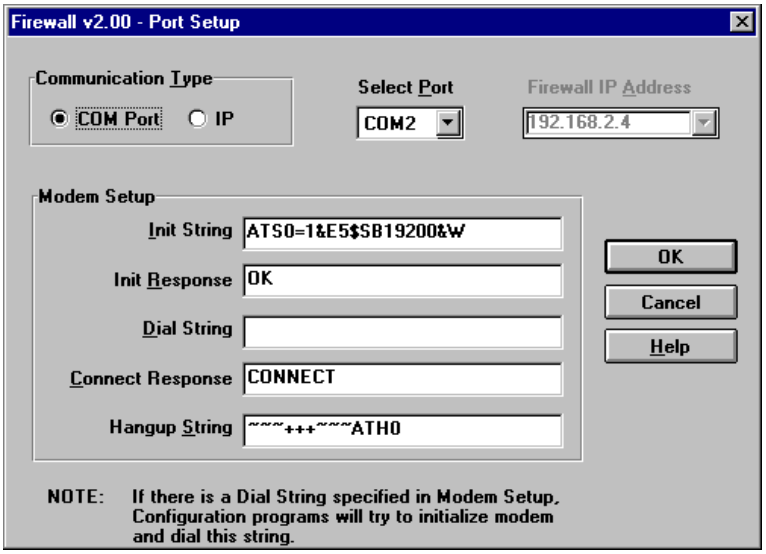
Connect the modem to your local telephone line.

Provide your telephone number to the person verifying your configuration.

3 At the main site, connect your local PC to a modem that is connected to a dial-up line.

4 Install the Firewall software on the local PC. When installed, click **Start | Programs | Firewall | Configuration Port Setup**, or double click on the **Configuration Port** icon in the Firewall program group.

5 The **Firewall Setup** dialog box is displayed.



Verify that the **Communication Type** is set for **COM Port** and the **Select Port** field is set for the COM port of your local PC.

In the **Dial String** field, enter the AT command for dialing (ATDT) plus the phone number of the remote ProxyServer.

If your Modem Initialization String, Initialization Response, or Connect Response values are different than the defaults in the dialog box, refer to your modem user documentation and change the default values to match those required by your modem.

Click **OK** when you are satisfied with your selections.

6 Run the Firewall Configuration program. Click **Start | Programs | Firewall | Firewall Configuration**, or double click on the **Firewall Configuration** icon in the Firewall program group.

7 The **Dialing Router** dialog box is displayed while software is dialing the remote Firewall.

8 The **Reading Setup** dialog box is displayed.

9 The **Firewall Setup** menu is displayed. This is the dialog box of the remote Firewall. Refer to the online Help provided with your software for a description of each dialog box and field within a dialog box.

10 After you have changed the configuration of the remote Firewall, click **Download Setup** to update the configuration. The remote Firewall will be brought down, the new configuration written to the unit, and the unit will reboot.

11 Click **Exit** when the downloading is complete.

12 The **Hangup connection with Router?** dialog box is displayed

Click **Yes** to disconnect the phone connection to the remote site.

13 If the same telephone number is not going to be used again in the immediate future, you may want to remove it from the Port Setup dialog box.

14 At the remote site, reconnect the Firewall to the serial port of the PC and from the Firewall program group double click on the **Firewall Configuration** icon to verify that the Firewall is running.

LAN-Based

The LAN-based remote configuration requires a Windows Sockets compliant TCP/IP stack. TCP/IP protocol software must be installed and functional before the configuration program can be used.

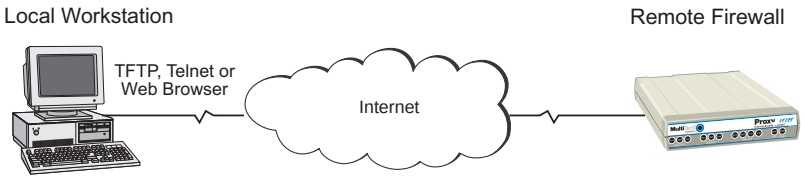


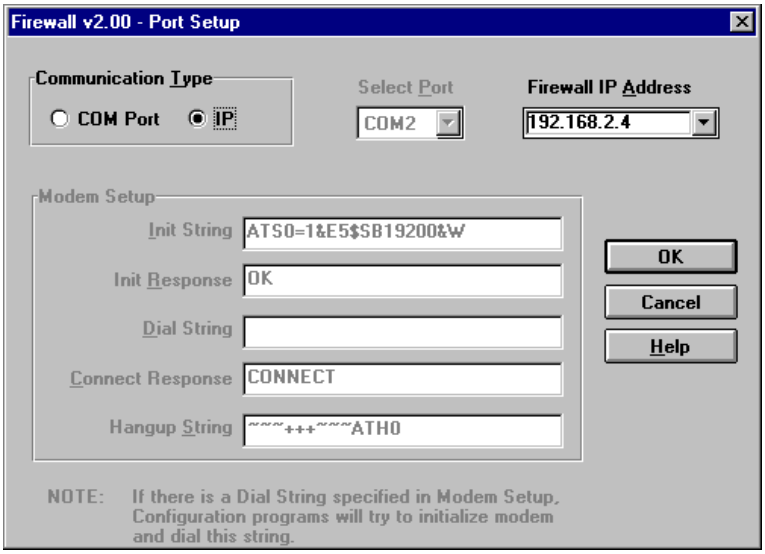
Figure 5-2. LAN-Based Remote Configuration

1 You must assign an Internet (IP) address for the PC and for each node that will be managed by the configuration program. Refer to the protocol software documentation for instructions on how to set the IP addresses.

Once you have completed this step, you should be able to use the protocol Ping command for the PC host name. You should also test the network interface configuration by Pinging another TCP/IP device that is connected to the network.

2 Install the Firewall software on the local PC. When installed click **Start | Programs | Firewall | Configuration Port Setup**, or double click on the **Configuration Port Setup** icon in the Firewall program group.

3 The Firewall Setup dialog box is displayed.



Verify that the **Communication Type** field is set **IP.**

In the **Router IP Address** field, enter the IP address of the remote Firewall.

4 Click **OK** when you are satisfied with your selections.

5 Run the Firewall Configuration program. Click **Start | Programs | Firewall | Firewall Configuration**, or double click on the **Firewall Configuration** icon in the Firewall program group.

6 The **Firewall Setup** dialog box is displayed. This is the dialog box of the remote Firewall. Refer to the online Help provided with your Firewall for the definition of each dialog box and field within a dialog box.

7 After you have changed the configuration of the remote Firewall, click **Download Setup** to update the configuration. The remote Firewall will be brought down, the new configuration written to the unit, and the unit will reboot.

8 Click **Exit** when the downloading is complete.

9 Double click on the **Firewall Configuration** icon in the Firewall program group to verify that the ProxyServer is running.

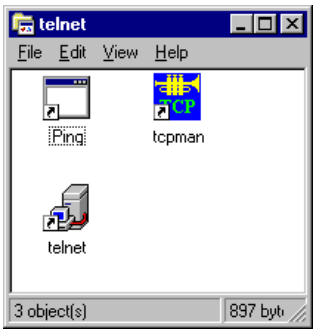
Remote Management

This section describes typical client applications that can be used to configure the ProxyServer remotely. It is important to note that although any subsequent changes to configuration can be made using these applications, the initial setup and configuration of the ProxyServer must be done on the local PC, using the ProxyServer software provided with your unit.

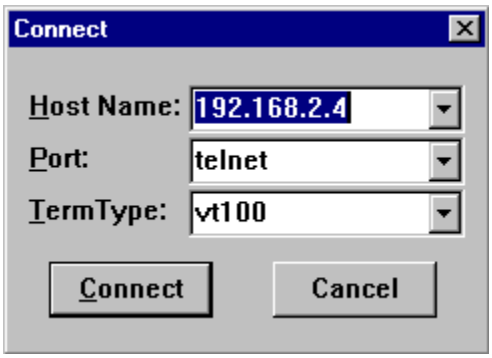
Although establishing access to the ProxyServer varies between applications, the configuration functions mirror those of the ProxyServer software. For more information on ProxyServer software, refer to Chapter 4 - Proxy Server Software.

Telnet

A typical Telnet client application is described in this chapter. The Firewall has a built-in Telnet Server that enables Telnet client PCs to access the ProxyServer. A typical Telnet client is allowed to configure the ProxyServer and WAN devices. A typical TCP/IP program group is shown below with a Tcpman icon and a Telnet icon.



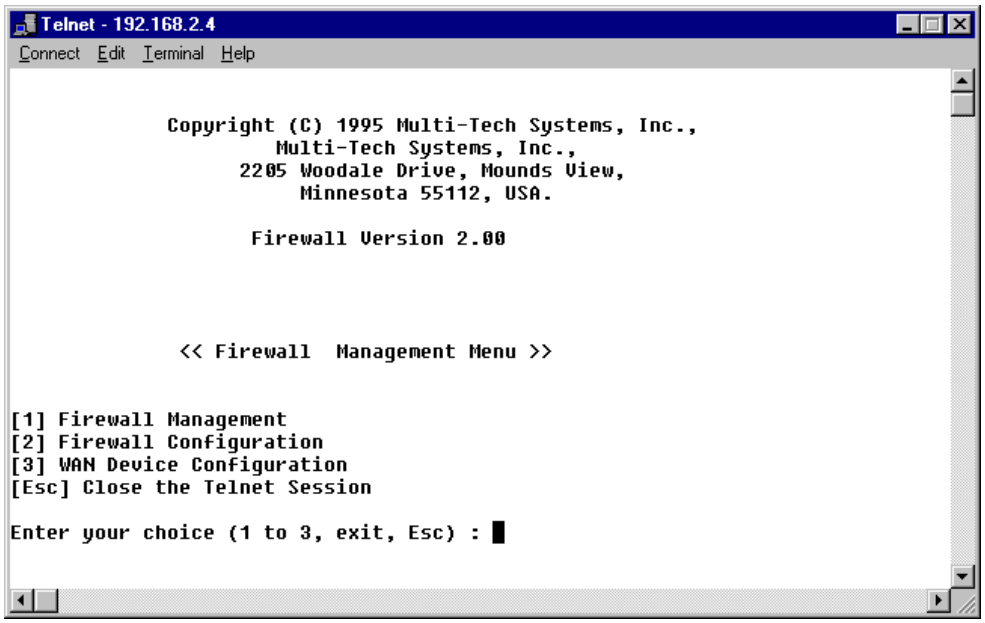
The TCP/IP stack has to be loaded before the Telnet client (a Windows application) will run, and the Telnet Server option has to be selected from the Applications Setup dialog box using Firewall Configuration (see Chapter 4 - Applications). Double click on the **Telnet** icon (or shortcut) and a blank Telnet screen is displayed. Click **Connect | Remote System** and the Connect dialog box is displayed. Select (or enter) a **Host Name** (the IP address of the ProxyServer). In this example, the Host Name is 192.168.2.4.



When you enter a valid Host Name (IP address) and click on **Connect**, you are immediately connected to the target ProxyServer and the **Firewall Management Menu** screen is displayed.

Firewall Management Menu

The Firewall Management Menu provides two basic options: Firewall Configuration and WAN Device Configuration. A further option enables you to close the Telnet session from this menu by pressing the Esc key.


Telnet - 192.168.2.4
Connect Edit Terminal Help
Copyright (C) 1995 Multi-Tech Systems, Inc.,
Multi-Tech Systems, Inc.,
2205 Woodale Drive, Mounds View,
Minnesota 55112, USA.
Firewall Version 2.00
<< Firewall Management Menu >>
[1] Firewall Management
[2] Firewall Configuration
[3] WAN Device Configuration
[Esc] Close the Telnet Session
Enter your choice (1 to 3, exit, Esc) :

Firewall Management

Selecting **Option 1** displays the **Firewall Management** menu with options that allow you to view statistics for IP, TCP, ARP, RARP, ICMP, UDP, WAN and PPP. In addition, you can access system information.

For more details on Firewall management, refer to Chapter 4 - Firewall Software, and the on-line helps.

Firewall Configuration

Selecting **Option 2** displays the **Firewall Configuration** menu with options that enable you to configure ProxyServer parameters and download settings.

For more details on Firewall configuration, refer to Chapter 4 - Firewall Software, and the on-line helps.

WAN Device Configuration

Selecting **Option 3** displays the **WAN Device Configuration** options, which enable you to gain direct access to the DCE device on the WAN port.

WEB Management

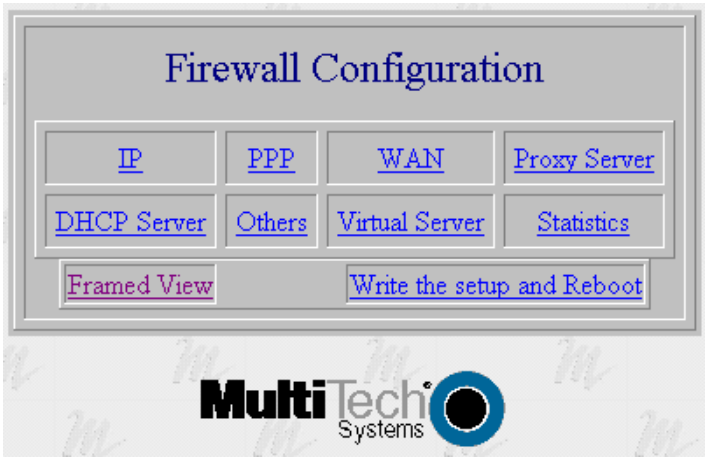
The ProxyServer can be accessed, via a standard web-browser, from anywhere on the connected Internet. In order to provide this support, the **WEB Server** option has to be enabled in the **Applications Setup** dialog box (see Chapter 4 - Firewall Software, Applications).

Once enabled, users can access the ProxyServer by entering its IP address in the destination field of their web browser. The following screen appears.

Address http://192.168.2.4/
FIREWALL
To configure this Firewall you should login as supervisor and enter Firewall password.
MultiTech Systems
2205 Woodale Drive --- Mounds View, MN 55112 --- United States
TEL: (612) 785-3500 or (800) 328-9717 --- FAX: (612) 785-9874 --- BBS: (612) 785-3702 or (800) 392-2432

Click on the word 'login' to log in to the ProxyServer configuration program. The **Enter Network Password** screen is displayed.

Type **supervisor** in the **User Name** field (no password needed) and click **OK**. The **Firewall Configuration** screen is displayed.



From this screen you can access all the configuration options. Refer to Chapter 4 - Firewall Software, for a description of the various options.

ProxyServer
Internet Access / Firewall

Chapter 6 - Warranty, Service and Tech Support

MultiTech® Systems

Introduction

This chapter starts out with statements about your Dual Ethernet ProxyServer 2-year warranty. The next section, Tech Support, should be read carefully if you have questions or problems with your ProxyServer. It includes the technical support telephone numbers, space for recording your product information, and an explanation of how to send in your ProxyServer should you require service. The final three sections explain how to use our bulletin board service (BBS), and get support through CompuServe and the Internet.

Limited Warranty

Multi-Tech Systems, Inc. (“MTS”) warrants that its products will be free from defects in material or workmanship for a period of two years from the date of purchase, or if proof of purchase is not provided, two years from date of shipment. MTS MAKES NO OTHER WARRANTY, EXPRESSED OR IMPLIED, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED. This warranty does not apply to any products which have been damaged by lightning storms, water, or power surges or which have been neglected, altered, abused, used for a purpose other than the one for which they were manufactured, repaired by the customer or any party without MTS’s written authorization, or used in any manner inconsistent with MTS’s instructions.

MTS’s entire obligation under this warranty shall be limited (at MTS’s option) to repair or replacement of any products which prove to be defective within the warranty period, or, at MTS’s option, issuance of a refund of the purchase price. Defective products must be returned by Customer to MTS’s factory transportation prepaid.

MTS WILL NOT BE LIABLE FOR CONSEQUENTIAL DAMAGES AND UNDER NO CIRCUMSTANCES WILL ITS LIABILITY EXCEED THE PURCHASE PRICE FOR DEFECTIVE PRODUCTS.

On-line Warranty Registration

To register your ProxyServer on-line, click on the following link:

http://www.multitech.com/register

Tech Support

Multi-Tech has an excellent staff of technical support personnel available to help you get the most out of your Multi-Tech product. If you have any questions about the operation of this unit, call 1-800-972-2439. Please fill out the ProxyServer information (below), and have it available when you call. If your ProxyServer requires service, the tech support specialist will guide you on how to send in your ProxyServer (refer to the next section).

Recording ProxyServer Information

Please fill in the following information on your Multi-Tech ProxyServer. This will help tech support in answering your questions. (The same information is requested on the Warranty Registration Card.)

Model No.: _____
Serial No.: _____
Software Version: _____

The model and serial numbers are on the bottom of your ProxyServer.

Please note the type of external link device that is connected to your ProxyServer before calling tech support. Also, note the status of your ProxyServer including LED indicators, screen messages, diagnostic test results, DIP-Switch settings, problems with a specific application, etc. Use the space below to note the ProxyServer status:

_____

_____

_____

_____

_____

_____

_____

_____

Service

If your tech support specialist decides that service is required, your ProxyServer may be sent (freight prepaid) to our factory. Return shipping charges will be paid by Multi-Tech Systems.

Include the following with your ProxyServer:

- a description of the problem.
- return billing and return shipping addresses.
- contact name and phone number.
- check or purchase order number for payment if the ProxyServer is out of warranty. (Check with your technical support specialist for the standard repair charge for your ProxyServer).
- if possible, note the name of the technical support specialist with whom you spoke.

If you need to inquire about the status of the returned product, be prepared to provide the **serial number** of the product sent.

Send your ProxyServer to this address:

MULTI-TECH SYSTEMS, INC.

2205 WOODALE DRIVE

MOUNDS VIEW, MINNESOTA 55112

ATTN: SERVICE OR REPAIRS

You should also check with the supplier of your ProxyServer on the availability of local service and/or loaner units in your part of the country.

The Multi-Tech BBS

For customers who do not have Internet access, Multi-Tech maintains a bulletin board system (BBS). Information available from the BBS includes new product information, product upgrade files, and problem-solving tips. The phone number for the Multi-Tech BBS is (800) 392-2432 (USA and Canada) or (612) 785-3702 (international and local).

The BBS can be accessed by any asynchronous modem operating at 1200 bps to 56K bps at a setting of 8 bits, no parity, and 1 stop bit (8-N-1).

To Log on to the Multi-Tech BBS

1. Set your communications program to **8-N-1**.
2. Dial our BBS at (800) 392-2432 (USA and Canada) or (612) 785-3702 (international and local).
3. At the prompts, type your first name, last name, and password; then press ENTER. If you are a first time caller, the BBS asks if your name is spelled correctly. If you answer yes, a questionnaire appears. You must complete the questionnaire to use the BBS on your first call.
4. Press ENTER until the Main Menu appears. From the Main Menu you have access to two areas: the Files Menu and News. For help on menu commands, type **?**.

To Download a File

If you know the file name

1. From the Main Menu, type **F** to access the Files Menu, then type **D**.
2. Enter the name of the file you wish to download from the BBS.
3. If a password is required, enter the password.
4. Answer **Y** or **N** to the automatic logoff question.
5. Select a file transfer protocol by typing the indicated letter, such as **Z** for Zmodem (the recommended protocol).
6. If you select Zmodem, the transfer will begin automatically. If you select another protocol, you may have to initiate the transfer yourself. (In most data communications programs, the PAGE DOWN key initiates the download.)
7. When the download is complete, press ENTER to return to the File Menu.
8. To exit the BBS, type **G** and press ENTER.

If you don’t know the file name

1. From the Main Menu, type **F** to access the Files Menu. For a list of file areas, type **L**, press ENTER, then type **L** and press ENTER again. (If you do not type the second *L*, you will list all of the files on the BBS.)
2. Mark each file area you would like to examine by typing its list number and pressing ENTER.
3. Enter **L** to list all the files in the selected file areas. Enter **C** to go forward in the file list and **P** to go back.
4. To mark one or more files for download, type **M**, press ENTER, type the list numbers of the files, and press ENTER again.

5. Enter **D**. You will see a list of the files you have marked. Enter **E** if you would like to edit the list; otherwise enter **D** again to start the download process.
6. Select a file transfer protocol by typing the indicated letter, such as **Z** for Zmodem (the recommended protocol).
7. If you select Zmodem, the file will transfer automatically. If you select another protocol, you may have to initiate the transfer yourself. (In most data communications programs, the PAGE DOWN key initiates the download.)
8. When the download is complete, press ENTER to return to the File Menu.
9. To exit the BBS, type **G** and press ENTER.

About the Internet

Multi-Tech is a commercial user on the Internet, and we retrieve messages from our customers on a periodic basis. If you prefer to receive technical support via the Internet, you can contact Tech Support at the following address:

http://www.multitech.com/_forms/email_tech_support.htm

Multi-Tech's presence includes a Web site at:

http://www.multitech.com

and an ftp site at:

ftp://ftp.multitech.com

About the Multi-Tech Fax-Back Service

Multi-Tech's fax-back system provides 24-hour access to sales, marketing, and technical literature. Dial 612-717-5888, follow the voice prompts, and request document number 10 for a catalog of available documents. For convenience, have your fax number handy: _____. From the catalog of available documents, you can order newsletters, white papers, press releases, etc. from the sales and marketing index (pages 1-4), or order basic modem operation and troubleshooting guides from the technical support and engineering index. Just enter the applicable FB Doc. # from the left column of the catalog.

ProxyServer
Internet Access / Firewall

Appendixes

MultiTech® Systems

Appendix A - TCP/IP (Transmission Control Protocol/ Internet Protocol) Description

TCP/IP is a protocol suite and related applications developed for the U.S. Department of Defense in the 1970s and 1980s specifically to permit different types of computers to communicate and exchange information with one another. TCP/IP is currently mandated as an official U.S. Department of Defense protocol and is also widely used in the UNIX community.

Before you install TCP/IP on your network, you need to establish your Internet addressing strategy. First, choose a domain name for your company. A domain name is the unique Internet name, usually the name of your business, that identifies your company. For example, Multi-Tech's domain name is multitech.com (.com indicates this is a commercial organization; .edu denotes educational organizations, .gov denotes government organizations). Next, determine how many IP addresses you'll need. This depends on how many individual network segments you have, and how many systems on each segment need to be connected to the Internet. You'll need an IP address for each network interface on each computer and hardware device.

IP addresses are 32 bits long and come in two types: network and host. Network addresses come in five classes: A, B, C, D, and E. Each class of network address is allocated a certain number of host addresses. For example, a class B network can have a maximum of 65,534 hosts, while a class C network can have only 254. The class A and B addresses have been exhausted, and the class D and E addresses are reserved for special use. Consequently, companies now seeking an Internet connection are limited to class C addresses.

Early IP implementations ran on hosts commonly interconnected by Ethernet local area networks (LAN). Every transmission on the LAN contains the local network, or medium access control (MAC), address of the source and destination nodes. The MAC address is 48-bits in length and is non-hierarchical; MAC addresses are never the same as IP addresses.

When a host needs to send a datagram to another host on the same network, the sending application must know both the IP and MAC addresses of the intended receiver. Unfortunately, the IP process may not know the MAC address of the receiver. The Address Resolution Protocol (ARP), described in RFC 826 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc826.txt) provides a mechanism for a host to determine a receiver's MAC address from the IP address. In the process, the host sends an ARP packet in a frame containing the MAC broadcast address; and then the ARP request advertises the destination IP address and asks for the associated MAC address. The station on the LAN that recognizes its own IP address will send an ARP response with its own MAC address. An ARP message is carried directly in an IP datagram.

Other address resolution procedures have also been defined, including those which allow a diskless processor to determine its IP address from its MAC address (Reverse ARP, or RARP), provides a mapping between an IP address and a frame relay virtual circuit identifier (Inverse ARP, or InARP), and provides a mapping between an IP address and ATM virtual path/channel identifiers (ATMARP).

The TCP/IP protocol suite comprises two protocols that correspond roughly to the OSI Transport and Session Layers; these protocols are called the Transmission Control Protocol and the User Datagram Protocol (UDP). Individual applications are referred to by a port identifier in TCP/UDP messages. The port identifier and IP address together form a "socket". Well-known port numbers on the server side of a connection include 20 (FTP data transfer), 21 (FTP control), 23 (Telnet), 25 (SMTP), 43 (whois), 70 (Gopher), 79 (finger), and 80 (HTTP).

TCP, described in RFC 793 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc793.txt) provides a virtual circuit (connection-oriented) communication service across the network. TCP includes rules for formatting messages, establishing and terminating virtual circuits, sequencing, flow control, and error correction. Most of the applications in the TCP/IP suite operate over the "reliable" transport service provided by TCP.

UDP, described in RFC 768 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc768.txt) provides an end-to-end datagram (connectionless) service. Some applications, such as those that involve a simple query and response, are better suited to the datagram service of UDP because there is no time lost to virtual circuit establishment and termination. UDP's primary function is to add a port number to the IP address to provide a socket for the application.

The Application Layer protocols are examples of common TCP/IP applications and utilities, which include:

- Telnet (Telecommunication Network): a virtual terminal protocol allowing a user logged on to one TCP/IP host to access other hosts on the network, described in RFC 854 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc854.txt).
- FTP: the File Transfer Protocol allows a user to transfer files between local and remote host computers per RFC 959 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc959.txt).
- Archie: a utility that allows a user to search all registered anonymous FTP sites for files on a specified topic.
- Gopher: a tool that allows users to search through data repositories using a menu-driven, hierarchical interface, with links to other sites, per RFC 1436 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1436.txt).
- SMTP: the Simple Mail Transfer Protocol is the standard protocol for the exchange of electronic mail over the Internet, per RFC 821 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc821.txt).
- HTTP: the Hypertext Transfer Protocol is the basis for exchange of information over the World Wide Web (WWW). Various versions of HTTP are in use over the Internet, with HTTP version 1.0, per RFC 1945 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1945.txt) being the most current.
- HTML: WWW pages are written in the Hypertext Markup Language (HTML), an ASCII-based, platform-independent formatting language, per RFC 1866 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1866.txt).
- Finger: used to determine the status of other hosts and/or users, per RFC 1288 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1288.txt).
- POP: the Post Office Protocol defines a simple interface between a user's mail reader software and an electronic mail server; the current version is POP3, described in RFC 1460 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1460.txt).
- DNS: the Domain Name System defines the structure of Internet names and their association with IP addresses, as well as the association of mail, name, and other servers with domains.
- SNMP: the Simple Network Management Protocol defines procedures and management information databases for managing TCP/IP-based network devices. SNMP, defined by RFC 1157 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1157.txt) is widely deployed in local and wide area network. SNMP Version 2 (SNMPv2), per RFC 1441 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1441.txt) adds security mechanisms that are missing in SNMP, but is also more complex.
- Ping: a utility that allows a user at one system to determine the status of other hosts and the latency in getting a message to that host. Ping uses ICMP Echo messages.
- Whois/NICNAME: Utilities that search databases for information about Internet domain and domain contact information, per RFC 954 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc954.txt).
- Traceroute: a tool that displays the route that packets will take when traveling to a remote host.

Internet Protocol (IP)

IP is the Internet standard protocol that tracks Internetwork node addresses, routes outgoing messages and recognizes incoming messages, allowing a message to cross multiple networks on the way to its final destination. The IPv6 Control Protocol (IPV6CP) is responsible for configuring, enabling, and disabling the IPv6 protocol modules on both ends of the point-to-point link. IPV6CP uses the same packet exchange mechanism as the Link Control Protocol (LCP). IPV6CP packets are not exchanged until PPP has reached the Network-Layer Protocol phase. IPV6CP packets received before this phase is reached are silently discarded. (See also TCP/IP.)

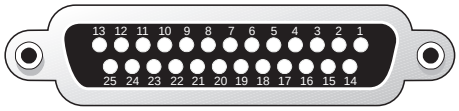
Before you install TCP/IP on your network, you need to establish your Internet addressing strategy. You first choose a domain name for your company. A domain name is the unique Internet name, usually the name of your business, that identifies your company. For example, Multi-Tech's domain name is multitech.com (where .com indicates this is a commercial organization; .edu denotes educational organizations, .gov denotes government organizations). Next, you determine how many IP addresses you'll need. This depends on how many individual network segments you have, and how many systems on each segment need to be connected to the Internet. You need an IP address for each network interface on each computer and hardware device.

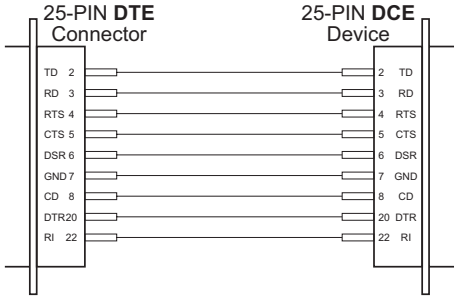
IP addresses are 32 bits long and come in two types: network and host. Network addresses come in five classes: A, B, C, D, and E. Each class of network address is allocated a certain number of host addresses. For example, a class B network can have a maximum of 65,534 hosts, while a class C network can have only 254. The class A and B addresses have been exhausted, and the class D and E addresses are reserved for special use. Consequently, companies now seeking an Internet connection are limited to class C addresses. The current demand for Internet connections will exhaust the current stock of 32-bit IP addresses. In response, Internet architects have proposed the next generation of IP addresses, Ipng (IP Next Generation). It will feature 16-byte addressing, surpassing the capacities of 32-bit IP. Still in its design phase, IPng is not expected to be widely deployed before late 1997.

An IP address can serve only a single physical network. Therefore, if your organization has multiple physical networks, you must make them appear as one to external users. This is done via "subnetting", a complex procedure best left to ISPs and others experienced in IP addressing. Since IP addresses and domain names have no inherent connection, they are mapped together in databases stored on Domain Name Servers (DNS). If you decide to let an Internet Service Provider (ISP) administer your DNS server, the ISP can assist you with the domain name and IP address assignment necessary to configure your company's site-specific system information. Domain names and IP addresses are granted by the InterNIC. To check the availability of a specific name or to obtain more information, call the InterNIC at (703)742-4777, or visit the InterNIC web site at http://www.internic.com.

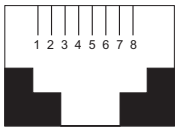
Appendix B - Cabling Diagrams

WAN Port Cable (RS-232/V.35)



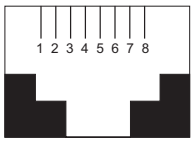


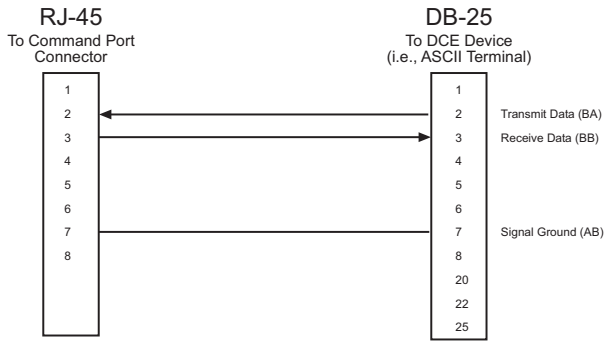
Ethernet Cables (10BaseT)



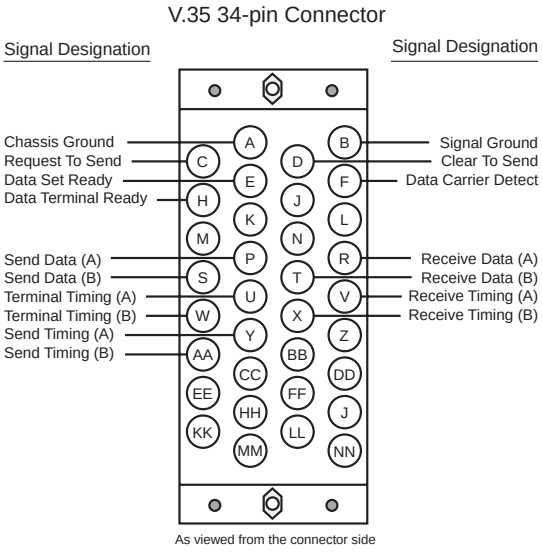
Pin	Circuit	Signal Name
1	TD+	Data Transmit Positive
2	TD-	Data Transmit Negative
3	RD+	Data Receive Positive
6	RD-	Data Receive Negative

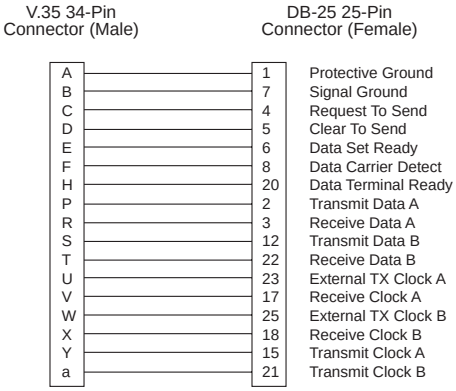
Command Port Cable (RJ-45)





DB-25 (RS-232) to V.35 Adapter

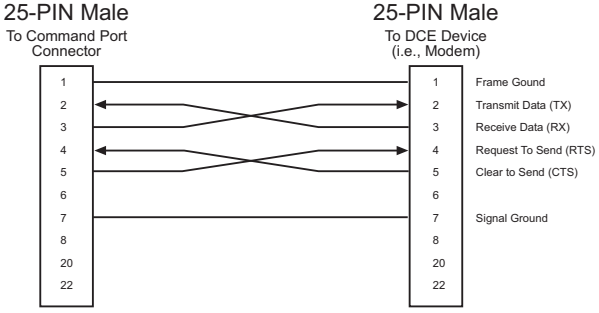

V.35 34-pin Connector
Signal Designation
Signal Designation
Chassis Ground
Request To Send
Data Set Ready
Data Terminal Ready
Send Data (A)
Send Data (B)
Terminal Timing (A)
Terminal Timing (B)
Send Timing (A)
Send Timing (B)
Signal Ground
Clear To Send
Data Carrier Detect
Receive Data (A)
Receive Data (B)
Receive Timing (A)
Receive Timing (B)
A B C D E F H J K L M N P R S T U V W X Y Z AA BB CC DD EE FF HH J KK LL MM NN
As viewed from the connector side


V.35 34-Pin Connector (Male)
DB-25 25-Pin Connector (Female)
A 1 Protective Ground
B 7 Signal Ground
C 4 Request To Send
D 5 Clear To Send
E 6 Data Set Ready
F 8 Data Carrier Detect
H 20 Data Terminal Ready
P 2 Transmit Data A
R 3 Receive Data A
S 12 Transmit Data B
T 22 Receive Data B
U 23 External TX Clock A
V 17 Receive Clock A
W 25 External TX Clock B
X 18 Receive Clock B
Y 15 Transmit Clock A
a 21 Transmit Clock B

* The RS-232C Interface circuits have been designed to meet the electrical specifications given in EIA (Electronic Industries Association) RS-232C and CCITT (Consultive Committee International Telegraph and Telephone) V.24 Standards

** When configured for V.35 interface operation on the link, the V.35 adapter cable should be used. This cable uses a 25-pin female connector at one end and a 34-pin winchester male connector at the other.

Remote Configuration Cable


25-PIN Male
To Command Port Connector
25-PIN Male
To DCE Device (i.e., Modem)
1 2 3 4 5 6 7 8 20 22
1 2 3 4 5 6 7 8 20 22
Frame Gound
Transmit Data (TX)
Receive Data (RX)
Request To Send (RTS)
Clear to Send (CTS)
Signal Ground

Appendix C - Regulatory Information

FCC Declaration

NOTE: This equipment has been tested and found to comply with the limits for a **Class A** digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Modem CE Mark EMC and Safety Compliance

The CE mark is affixed to the enclosed MultiTech product to confirm compliance with the following European Community Directives:

Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of Member States relating to electromagnetic compatibility;

and

Council Directive 73/23/EEC of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits;

both amended by

Council Directive 93/68/EEC of 22 July 1993 on the harmonization of CE marking requirements.

ProxyServer
Internet Access / Firewall

Glossary

MultiTech® Systems

A

Access: The T1 line element made up of two pairs of wire that the telephone company brings to the customer premises. The Access portion ends with a connection at the local telco (LEC or RBOC).

Accunet Spectrum of Digital Services (ASDS): The AT&T 56K bps leased (private) line service. Similar to services of MCI and Sprint. ASDS is available in nx56/64K bps, where n=1, 2, 4, 6, 8, 12.

ACK (ACKnowledgement code) (pronounced "ack"): A communications code sent from a receiving modem to a transmitting modem to indicate that it is ready to accept data. It is also used to acknowledge the error-free receipt of transmitted data. Contrast with NAK.

Adaptive Differential Pulse Code (ADCPM): In multimedia applications, a technique in which pulse code modulation samples are compressed before they are stored on a disk. ADCPM, an extension of the PCM format, is a standard encoding format for storing audio information in a digital format. It reduced storage requirements by storing differences between successive digital samples rather than full values.

Address: A numbered location inside a computer. It's how the computer accesses its resources, like a video card, serial ports, memory, etc.

AMI line coding: One of two common methods of T1 line coding (with B8ZS). AMI line coding places restrictions on user data (B8ZS does not).

Analog signal: A waveform which has amplitude, frequency and phase, and which takes on a range of values between its maximum and minimum points.

Analog Transmission: One of two types of telecommunications which uses an analog signal as a carrier of voice, data, video, etc. An analog signal becomes a carrier when it is modulated by altering its phase, amplitude and frequency to correspond with the source signal. Compare with digital transmission.

Application Program Interface (API): A software module created to allow dissimilar, or incompatible applications programs to transfer information over a communications link. APIs may be simple or complex; they are commonly required to link PC applications with mainframe programs.

ASCII (American Standard Code for Information Interchange) (pronounced "askey"): A binary code for data that is used in communications and in many computers and terminals. The code is used to represent numbers, letters, punctuation and control characters. The basic ASCII code is a 7-bit character set which defines 128 possible characters. The extended ASCII file provides 255 characters.

Asynchronous Transfer Mode (ATM): A very high-speed method of transmission that uses fixed-size cells of 53 bytes to transfer information over fiber; also known as cell relay.

AT Commands: A standard set of commands used to configure various modem parameters, establish connections and disconnect. The "AT" is used to get the "attention" of the modem before the actual command is issued.

Availability: The measure of the time during which a circuit is ready for use; the complement of circuit "outage" (100% minus % outage = % available).

B

B7ZS (Bipolar 7 Zero Suppression) line coding: One method of T1 line coding (see also "B8ZS" and "AMI"). B7ZS line coding does not place restrictions on user data (AMI does).

B8ZS (Bipolar 8 Zero Suppression) line coding: One of two common methods of T1 line coding (with AMI). B8ZS line coding does not place restrictions on user data (AMI does). A coding method used to produce 64K bps "clear" transmission. (See also "B7ZS" and "AMI" line coding)

Backbone: 1. A set of nodes and their interconnecting links providing the primary data path across a network. 2. In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges. A backbone may be configured as a bus or as a ring. 3. In a wide area network, a high-speed link to which nodes or data switching exchanges (DSEs) are connected. 4. A common distribution core that provides all electrical power, gases, chemicals, and other services to the sectors of an automated wafer processing system.

Background: An activity that takes place in the PC while you are running another application. In other words, the active user interface does not correspond to the 'background' task.

Bandwidth: The transmission capacity of a computer channel, communications line or bus. It is expressed in cycles per second (hertz), the bandwidth being the difference between the lowest and highest frequencies transmitted. The range of usable frequencies that a transmission medium will pass without unacceptable attenuation or distortion. Bandwidth is a factor in determining the amount of information and the speed at which a medium can transmit data or other information.

Backward Explicit Congestion Notification (BECN): A bit that tells you that a certain frame on a particular logical connection has encountered heavy traffic. The bit provides notification that congestion-avoidance procedures should be initiated in the opposite direction of the received frame. See also FECN (Forward Explicit Congestion Notification).

Basic Rate Interface (BRI): An ISDN access interface type comprised of two B-channels each at 64K bps and one D-channel at 64K bps (2B+D).

Bell Operating Companies (BOC): The family of corporations created during the divestiture of AT&T. BOCs are independent companies which service a specific region of the US. Also called Regional Bell Operating Companies (RBOCs).

Bell Pub 41450: The Bell publication defining requirements for data format conversion, line conditioning, and termination for direct DDS connection.

Bell Pub 62310: The Bell publication defining requirements for data format conversion, line conditioning, and termination for direct DDS connection.

Binary Synchronous Communication (BSC): A form of telecommunication line control that uses a standard set of transmission control characters and control character sequences, for binary synchronous transmission of binary-coded data between stations.

Bit (Binary digIT): A bit is the basis of the binary number system. It can take the value of 1 or 0. Bits are generally recognized as the electrical charge generated or stored by a computer that represent some portion of usable information.

Bit Error Rate Test (BERT): A device or routine that measures the quality of data transmission. A known bit pattern is transmitted, and the errors received are counted and a BER (bit error rate) is calculated. The BER is the ratio of received bits in error relative to the total number of bits received, expressed in a power of 10.

Bit robbing: The use of the least significant bit per channel in every sixth frame for signaling. The line signal bits “robbed” from the speech part conveys sufficient pre-ISDN telephony signaling information with the remaining line signal bits providing sufficient line signaling bits for recreating the original sound. See “robbed bit signaling”.

Blue Alarm: An error indication signal consisting of all 1s indicating disconnection or attached device failure. Contrast “Red Alarm” and “Yellow Alarm”.

Bps (bits per second): A unit to measure the speed at which data bits can be transmitted or received. Bps differs from baud when more than one bit is represented by a single cycle of the carrier.

Bridges: 1. A functional unit that interconnects two local area networks that use the same logical link protocol but may use different medium access control protocols. 2. A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address. 3. In the connection of local loops, channels, or rings, the equipment and techniques used to match circuits and to facilitate accurate data transmission.

Buffer: A temporary storage register or Random Access Memory (RAM) used in all aspects of data communications which prevents data from being lost due to differences in transmission speed. Keyboards, serial ports, muxes and printers are a few examples of the devices that contain buffers.

Bus: A common channel between hardware devices either internally between components in a computer, or externally between stations in a communications network.

Byte: The unit of information a computer can handle at one time. The most common understanding is that a byte consists of 8 binary digits (bits), because that’s what computers can handle. A byte holds the equivalent of a single character (such as the letter A).

C

Call Setup Time: The time to establish a circuit-switched call between two points. Includes dialing, wait time, and CO/long distance service movement time.

Carrier Group Alarm (CGA): A T1 service alarm generated by a channel bank when an OOF condition occurs for a predefined length of time (usually 300mS to 2.5 seconds). The CGA causes the calls using a trunk to be dropped and for trunk conditioning to be applied.

Carrier signal: An analog signal with known frequency, amplitude and phase characteristics used as a transport facility for useful information. By knowing the original characteristics, a receiver can interpret any changes as modulations, and thereby recover the information.

CCITT (Consultative Committee for International Telephone and Telegraph): An advisory committee created and controlled by the United Nations and headquartered in Geneva whose purpose is to develop and to publish recommendations for worldwide standardization of telecommunications devices. CCITT has developed modem standards that are adapted primarily by PTT (post, telephone and telegraph) organizations that operate telephone networks of countries outside of the U.S. See also ITU.

Central Office (CO): The lowest, or most basic level of switching in the PSTN (public switched telephone network). A business PABX or any residential telephone connects to the PSTN at a central office.

Centrex: A multi-line service offered by operating telcos which provides, from the telco CO, functions and features comparable to those of a PBX for large business users. See also “Private Branch Exchange”, “Exchange”.

Channel: A data communications path between two computer devices. Can refer to a physical medium (e.g., UTP or coax), or to a specific carrier frequency.

Channel Bank: A device that acts as a converter, taking the digital signal from the T1 line into a phone system and converting it to the analog signals used by the phone system. A channel bank acts as a multiplexer, placing many slow-speed voice or data transactions on a single high-speed link.

Circuit-switched Network: A technology used by the PSTN that allocates a pair of conductors for the exclusive use of one communication path. Circuit switching allows multiple conversations on one talk path only if the end-users multiplex the signals prior to transmission.

Circuit Switching: The temporary connection of two or more communications channels using a fixed, non-shareable path through the network. Users have full use of the circuit until the connection is terminated.

Clear Channel: A transmission path where the full bandwidth is used (i.e., no bandwidth needed for signaling, carrier framing or control bits). A 64K bps digital circuit usually has 8K bps used for signaling. ISDN has two 64K bps circuits, and a 16K bps packet service of which part is used for signaling on the 64K channels.

Client-Server: In TCP/IP, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

Cluster Controller: A device that can control the input/output operations of more than one device connected to it. A cluster controller may be controlled by a program stored and executed in the unit, or it may be entirely controlled by hardware.

Committed Burst Size: The maximum number of bits that the frame relay network agrees to transfer during any measurement interval.

Committed Information Rate (CIR): An agreement a customer makes to use a certain minimum data transmission rate (in bps). The CIR is part of the frame relay service monthly billing, along with actual usage, that users pay to their frame relay service provider.

Compression: 1. The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks. 2. In SNA, the replacement of a string of up to 64-repeated characters by an encoded control byte to reduce the length of the data stream to the LU-LU session partner. The encoded control byte is followed by the character that was repeated (unless that character is the prime compression character). 3. In Data Facility Hierarchical Storage Manager, the process of moving data instead of allocated space during migration and recall in order to release unused space. 4. Contrast with decompression.

COMx Port: A serial communications port on a PC.

congestion: A network condition where there is too much data traffic. The ITU I.233 standard defines congestion managemennt in terms of speed and burstiness.

congestion notification: The function in frame relay that ensures that user data transmitted at a rate higher than the CIR are allowed to slow down to the rate of the available network bandwidth.

Consecutive Severely Errored Seconds (CSES): An error condition that occurs when from 3 to 9 SES (Severely Errored Seconds) are logged consecutively.

Customer Premise Equipment (CPE): The generic term for data comm and/or terminal equipment that resides at the user site and is owned by the user with the following exclusions: Over voltage protection equipment, inside wiring, coin operated or pay telephones, “company-official” equipment, mobile telephone equipment, “911” equipment, equipment necessary for the provision of communications for national defense, or multiplexing equipment used to deliver multiple channels to the customer.

D

D4: the T1 4th generation channel bank.

D4 channelization: Refers to the compliance with AT&T TR 62411 for DS1 frame layout.

D4 framing: The T1 format for framing in AT&T D-Series channel banks, in which there are 12 separate 193-bit frames in a super-frame. A D4 framing bit is used to identify the channel and the signaling frame. Signalling for voice channels is carried in-band for every channel, along with the encoded voice. See “robbed-bit signaling”.

Data Communications Equipment (DCE): Any device which serves as the portal of entry from the user equipment to a telecommunications facility. A modem is a DCE for the telephone network (PSTN) that is commonly on site at the user’s premises. Packet Switched Networks have another level of DCE which is most often located at a central office.

Data Link Connection Identifier (DLCI): One of the six components of a frame relay frame. Its purpose is to distinguish separate virtual circuits across each access connection. Data coming into a frame relay node is thus allowed to be sent across the interface to the specified “address”. The DLCI is confirmed and relayed to its destination, or if the specification is in error, the frame is discarded.

Dataphone Digital Service (DDS): A private line digital service that offers 2400, 4800, 9600 and 56K bps data rates on an inter-LATA basis by AT&T and on an intra-LATA basis by the BOCs.

Data Service Unit (DSU): A device that provides a digital data service interface directly to the data terminal equipment. The DSU provides loop equalization, remote and local testing capabilities, and a standard EIA/CCITT interface.

Dedicated Line: A communication line that is not switched. The term leased line is more common.

Default: This is a preset value or option in software packages, or in hardware configuration, that is used unless you specify otherwise.

Device driver: Software that controls how a computer communicates with a device, such as a printer or mouse.

Digital Cross-connect System (DCS): The CO device which splits and redistributes the T1 bandwidth. the DCS takes time slots from various T1 lines and alters them to provide the needed connectivity. DCS connections are made with software at an administrator’s workstation.

Digital Data: Information represented by discrete values or conditions (contrast “Analog Data”).

Digital Loopback: A technique used for testing the circuitry of a communications device. Can be initiated locally, or remotely (via a telecommunications device). The tested device decodes and encodes a received test message, then echoes the message back. The results are compared with the original message to determine if corruption occurred en route.

Digital PBX: A Private Branch Exchange that operates internally on digital signals. See also “Exchange”.

Digital Service, level 0 (DS0): The world-wide standard speed (64K bps) for digital voice conversation using PCM (pulse coded modulation).

Digital Service, level 1 (DS1): The 1.544M bps voice standard (derived from an older Bell System standard) for digitized voice transmission in North America. The 1.544M bps consists of 24 digitally-encoded 64K bps voice channels (north America) and 2.048M bps (30 channels) elsewhere.

Digital Signal: A discrete or discontinuous signal (e.g., a sequence of voltage pulses). Digital devices, such as terminals and computers, transmit data as a series of electrical pulses which have discrete jumps rather than gradual changes.

Digital Signaling Rates (DSn): A hierarchical system for transmission rates, where “DS0” is 64K bps (equivalent to ISDN B channel), and DS1 is 1.5 Mbps (equivalent to ISDN PRI).

Digital Transmission: A method of electronic information transmission common between computers and other digital devices. Analog signals are waveforms: a combination of many possible voltages. A computer’s digital signal may be only “high” or “low” at any given time. Therefore, digital signals may be “cleaned up” (noise and distortion removed) and amplified during transmission.

Digitize: To convert an analog signal to a digital signal.

DIP switch (pronounced “dip switch”): A set of tiny toggle switches, built into a DIP (dual in-line package), used for setting configurable parameters on a PCB (printed circuit board).

Driver: A software module that interfaces between the Operating System and a specific hardware device (e.g., color monitors, printers, hard disks, etc.). Also known as a device driver.

Drop and Insert: The process where a portion of information carried in a transmission system is demodulated (“Dropped”) at an intermediate point and different information is included (“Inserted”) for subsequent transmission.

DTE (Data Terminal Equipment): A term used to include any device in a network which generates, stores or displays user information. DTE is a telecommunications term which usually refers to PCs, terminals, printers, etc.

DTMF (Dual-Tone MultiFrequency): A generic push-button concept made popular by AT&T TouchTone.

E

E&M: A telephony trunking system used for either switch-to-switch, or switch-to-network, or computer/telephone system-to-switch connection.

EIA: The Electronics Industries Association is a trade organization in Washington, DC that sets standards for use of its member companies. (See RS-232, RS-422, RS530.)

Encapsulation: A technique used by network-layer protocols in which a layer adds header information to the protocol data unit from the preceding layer. Also used in “enveloping” one protocol inside another for transmission. For example, IP inside IPX.

Errored Seconds (ES): Any second of operation that all 1.544M bits are not received exactly as transmitted. Contrast “Error Free Seconds”.

Error Free Seconds (EFS): Any second of operation that all 1.544M bits are received exactly as transmitted. Contrast “Errored Seconds”.

ESF Error Event: A T1 error condition that is logged when a CRC-6 error or an Out-Of-Frame (OOF) error occurs.

Ethernet: A 10-megabit baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and transmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

Excess Zeros: A T1 error condition that is logged when more than 15 consecutive 0s or fewer than one 1 bit in 16 bits occurs.

Exchange: A unit (public or private) that can consist of one or more central offices established to serve a specified area. An exchange typically has a single rate of charges (tariffs) that has previously been approved by a regulatory group.

Exchange Area: A geographical area with a single uniform set of charges (tariffs), approved by a regulatory group, for telephone services. Calls between any two points within an exchange area are local calls. See also “Digital PBX”, “PBX”.

Exchange Termination (ET): The carrier’s local exchange switch. Contrast with “Loop Termination - LT”.

Explicit Congestion Management: The method used in frame relay to notify the terminal equipment that the network is overly busy. The use of FECN and BECN is called explicit congestion management. Some end-to-end protocols use FECN or BECN, but usually not both options together. With this method, a congestion condition is identified and fixed before it becomes critical. Contrast with “implicit congesion”.

Extended Super Frame (ESF): One of two popular formats for framing bits on a T1 line. ESF framing has a 24-frame super-frame, where robbed bit signaling is inserted in the LSB (bit 8 of the DS-0 byte) of frames 6, 12, 18 and 24. ESF has more T1 error measurement capabilities than D4 framing. Both ESF and B8ZS are typically offered to provide clear channel service.

F

Failed Seconds: A test parameter where the circuit is unavailable for one full second.

Failed Signal: A T1 test parameter logged when there are more than 9 SES (Severely Errored Seconds).

Fax (facsimile): Refers to the bit-mapped rendition of a graphics-oriented document (fax) or to the electronic transmission of the image over telephone lines (faxing). Fax transmission differs from data transmission in that the former is a bit-mapped approximation of a graphical document and, therefore, cannot be accurately interpreted according to any character code.

Firmware: A category of memory chips that hold their content without electrical power, they include ROM, PROM, EPROM and EEPROM technologies. Firmware becomes “hard software” when holding program code.

Foreground: The application program currently running on and in control of the PC screen and keyboard. The area of the screen that occupies the active window. Compare with “background”.

Fractional T1 (FT1): A digital data transmission rate between 56K bps (DS0 rate) and 1.544M bps (the full T1 rate - in North America). FT1 is typically provided on 4-wire (two copper pairs) UTP. Often used for video conferencing, imaging and LAN interconnection due to its low cost and relatively high speed. FT1 rates are offered in 64K bps multiples, usually up to 768K bps.

Frequency: A characteristic of an electrical or electronic signal which describes the periodic recurrence of cycles. Frequency is inversely proportional to the wavelength or pulse width of the signal (i.e., long wavelength signals have low frequencies and short wavelength signals yield high frequencies).

Foreign Exchange (FX): A CO trunk with access to a distant CO, allowing ease of access and flat-rate calls anywhere in the foreign exchange area.

Foreign Exchange Office (FXO): provides local telephone service from a CO outside of (“foreign” to) the subscriber’s exchange area. In simple form, a user can pick up the phone in one city and receive a tone in the foreign city. Connecting a POTS telephone to a computer telephony system via a T1 link requires a channel bank configured for the FX connection. To generate a call from the POTS set to the computer telephony system, a FXO connection must be configured.

Foreign Exchange Station (FXS): See FX, FXO. To generate a call from the computer telephony system to the POTS set, an FXS connection must be configured.

Forward Explicit Congestion Notification (FECN): A bit that tells you that a certain frame on a particular logical connection has encountered heavy traffic. The bit provides notification that congestion-avoidance procedures should be initiatedin the same direction of the received frame. See also BECN (Backward Explicit Congestion Notification).

Frame: A group of data bits in a specific format to help network equipment recognize what the bits mean and how to process them. The bits are sent serially, with a flag at each end signifying the start and end of the frame.

Frame Relay: A form of packet switching that uses small packets and that requires less error checking than other forms of packet switching. Frame relay is effective for sending “bursty” data at high speeds (56/64K, 256K, and 1024K bps) over wide area networks. Frame Relay specifications are defined by ANSI documents ANSI T1.602, T1.606, T1S1/90-175, T1S1/90-213, and T1S1/90-214. In using frame relay, blocks of information (frames) are passed across a digital network interface using a “connection number” that is applied to each frame to distinguish between individual frames.

Frame Relay Forum: A non-profit organization of 300+ vendors and service providers, based in Foster City, CA, that are developing and deploying frame relay equipment.

Frame Relay Implementors Forum: A group of companies supporting a common specification for frame relay connection to link customer premises equipment to telco network equipment. Their specification supports ANSI frame relay specs and defines extensions such as local management.

Frame Relay Access Device (FRAD): A piece of equipment that acts as a concentrator or frame assembler/ dissassember that can support multiple protocols and provide basic “routing” functions.

G

Gateway: 1. A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. 2. A network that connects hosts.

Graphical User Interface (GUI): A type of computer interface consisting of a visual metaphor of a real-world scene, often of a desktop. Within that scene are icons, representing actual objects, that the user can access and manipulate with a pointing device.

H

Handshaking: A process that two modems go through at the time of call setup to establish synchronization over the data communications link. It is a synchronization and negotiation process accomplished by the exchange of predefined, mutually recognized control codes.

High-level Data Link Control (HDLC): An ISO standard, bit-oriented data communications protocol that provides nearly error-free data transfers.

I

Hexadecimal: A base 16 numbering system used to represent binary values. Hex uses the numbers 0-9 and the letters A-F: usually notated by an “h” (e.g., “4CF h”, read “four charley fox, hex”). The result is that one hex digit represents a 4-bit value.

Implicit congestion management: A method of informing the terminal that the network is busy. This method relies on the end-system protocol to detect and fix the congestion problem. (TCP/IP is an example of a protocol using only implicit congestion management.) See also “explicit congestion management”.

In-band: Refers to the type of signalling over the conversion path on an ISDN call. Contrast “out-of-band”.

Insufficient Ones: A T1 error condition that is logged when fewer than one 1 in 16 0s or less than 12.5 % average 1s density is received.

Inter Exchange Carrier (IEC): The long distance company (LE) who’s central office provides the point of reference for T1 access. Any common carrier authorized by the FCC to carry customer transmissions between LATAs.

Internet: Refers to the computer network of many millions of university, government and private users around the world. Each user has a unique Internet Address.

Internet Address (IP Address): A unique 32-bit address for a specific TCP/IP host on a network. Normally printed in dotted decimal format (e.g., 129.128.44.227).

Internet Protocol (IP): A protocol used to route data from its source to its destination in an Internet enviroment. The Internet Protocol was designed to connect local area networks. Although there are many protocols that do this, IP refers to the global system of interconnecting computers. It is a highly distributed protocol (each machine only worries about sending data to the next step in the route).

Internetwork Packet Exchange (IPX): A NetWare communications protocol used to route messages from one node to another. IPX packets include network addresses and can be routed from one network to another. An IPX packet can occasionally get lost when crossing networks, thus IPX does not guarantee delivery of a complete message. Either the application has to provide that control, or NetWare's SPX protocol must be used.

Interoperable: Devices from different vendors that can exchange information using a standard's base protocol.

I/O Addresses: Locations within the I/O address space of your computer used by a device, such as an expansion card, a serial port, or an internal modem. The address is used for communication between software and a device.

IRQ Level (Interrupt Request Level): The notification a processor receives when another portion of the computer's hardware requires its attention. IRQs are numbered so that the device issuing the IRQ can be identified, and so IRQs can be prioritized.

ISA (Industry Standards Architecture) (pronounced "ice a"): The classic 8 or 16-bit architecture introduced with IBM's PC-AT computer.

ISDN (Integrated Services Digital Network): An International telecommunications standard for transmitting voice, video and data over a digital communications line. ISDN is a world-wide telecommunications service that uses digital transmission and switching technology to support voice and digital data communications. Frame relay was partially based on ISDN's data link layer protocol (LAPD). Frame relay can be used to transmit across ISDN services offering circuit-switched connection at 64K bps and higher speeds. Contrast Public Switched Telephone Network (PSTN).

ITU-TSS (formerly CCITT): International Telecommunications Union-Telecommunications Sector; the United Nations organization that prepares standards ("Recommendations") for resolving communications issues and problems.

J

No Entries.

K

Key Telephone System (KTS): Phone devices with multiple buttons that let you select incoming or outgoing CO phone lines directly. Similar in operation to a PBX, except with a KTS you don't have to dial a "9" for a call outside the building.

Key Service Unit (KSU): A small device containing the switching electronics for a business key telephone system (KTS).

Key Set: A telephone set with several buttons for call holding, line pickup, intercom, autodialing, etc. Also called a touchtone phone (Ericsson) and a KTS (Key Telephone Set).

L

LAPB: Link Access Procedure Balanced; based on the X.25 Layer 2 specification. A full-duplex point-to-point, bit-synchronous protocol commonly used as a data link control protocol to interface X.25 DTEs. LAPB is the link initialization procedure that establishes and maintains communications between the DTE and the DCE.

LAPD: Link Access Protocol for the D-Channel; based on the ISDN Q.921 specification. A full-duplex, point-to-point bit-synchronous link-level protocol for ISDN connections; different from LAPB in its framing sequence. Transmission is in units called "frames", and a frame may contain one or more X.25 packets.

Line Coding: The representation of 1s and 0s on a T1 line. The two methods of line coding commonly used, B8ZS and AMI, differ in the restrictions placed on user data. T1 line coding ensures that sufficient timing information is sent with the digital signal to ensure recovery of all the bits at the far end. Timing information on the T1 line is included in the form of 1s in the data stream; a long string of 0s in the data stream could cause problems recovering the data.

Line Termination (LT): The electronics at the ISDN network side of the user/network interface that complements the NT1 at the user side. The LT and the NT1 together provide the high-speed digital line signals required for BRI access.

Listed Directory Number (LDN): The main number assigned by the telco; the number listed in the telephone directory and also provided by Directory Assistance. Some devices can have more than one LDN, such as ISDN devices that have one LDN for voice and another LDN for data.

Local Area Network (LAN): 1. A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. 2. A LAN does not use store-and-forward techniques. 3. A network in which a set of devices are connected to one another for a communication and that can be connected to a larger network.

Local Access and Transport Area (LATA): A post-divestiture geographical area generally equivalent to a Standard Metropolitan Statistical Area. At divestiture, the territory served by the Bell system was divided into approximately 161 LATAs. The Bell Operating Companies (BOCs) provide Intra-LATA services.

Local Exchange Carrier (LEC): The local phone company which provides local (i.e., not long distance) transmission services. AKA “telco”. LECs provide T1 or FT1 access to LDCs (unless the T1 circuit is completely intra-LATA). Inter-LATA T1 circuits are made up of a combination of Access and Long Haul facilities.

Local Management Interface (LMI): A specification for frame relay equipment that defines status information exchange.

Local Loop: A transmission path, typically twisted-pair wire, between an individual subscriber and the nearest public telecommunications network switching center. The wires provide ISDN service, but require an NT1 at the user end and an LT at the network end. (AKA, “loop” or “subscriber loop”.)

Logical Link Control (LLC2): In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. The LLC2 protocol was developed by the IEEE 802 commitee and is common to all LAN standards.

Logical Unit (LU): A type of network accessible unit that enables end users to gain access to network resources and communicate with each other.

Long Haul: The T1 element that connects to the Access portion of the long distance company’s (LDC’s) central office. The LDC is commonly called the point of presence (POP). Each LDC has a number of POPs, located throughout the country. The LDC is also called an IEC (Inter Exchange Carrier).

Long Haul Communications: The type of phone call reaching outside of a local exchange (LE).

M

Management Information Base (MIB): A database of network management information used by the Common Management Information Protocol (CMIP) and the Simple Network Management Protocol (SNMP).

Megacom: An AT&T service with a normal WATS line (typically T1) between the customer premise and the AT&T serving class 4 CO are the customer’s responibility.

MegaLink: BellSouth’s leased T1 service.

Message: Associated with such terms as packet, frame, and segment. 1. In information theory, an ordered series of characters intended to convey information. 2. An assembly of characters and sometimes control codes that is transferred as an entry from an originator to one or more recipients.

Modem: A communications device that enables a computer to transmit information over a telephone line. It converts the computer’s digital signals into analog signals to send over a telephone line and converts them back to digital signals at the receiving end. Modems can be internal and fit into an expansion slot, or external and connect to a serial port.

Multiplexer (Mux): 1. A device that takes several input signals and combines them into a single output signal in such a manner that each of the input signals can be recovered. 2. A device capable of interleaving the events of two or more activities or capable of distributing the events of an interleaved sequence to the respective activities. 3. Putting multiple signals on a single channel.

Multiprotocol: A device that can interoperate with devices utilizing different network protocols.

Multithreading: The ability of a software system to be able to handle more than one transaction concurrently. This is contrasted to the case where a single transaction is accepted and completely processed befor the next transaction processing is started.

N

Nailed Connection: A permanent or dedicated circuit of a previously switched circuit or circuits.

Nailed-up Circuit: A semi-permanent circuit established through a circuit-switching facility for point-to-point connectivity.

NAK (Negative Acknowledgment): Communications code used to indicate that a message was not properly received, or that a terminal does not wish to transmit. Contrast with ACK.

Network: A group of computers connected by cables or other means and using software that enables them to share equipment, such as printers and disk drives to exchange information.

Node: Any point within a network which has been assigned an address.

O

Object-Oriented: A method for structuring programs as hierarchically organized classes describing the data and operations of objects that may interact with other objects.

Office Channel Unit - Data Port (OCU-DP): The CO channel bank used as the interface between the customer's DSU and the channel bank.

Off-hook: The condition of a device which has accessed a phone line (with or without using the line). In modem use, this is equivalent to a telephone handset being picked up. Dialing and transmission are allowed, but incoming calls are not answered. Contrast "on-hook".

Off Premise Extension (OPX): An extension or phone that terminates in a location other than that of the PBX. Commonly used to provide a corporate member with an extension of the PBX at home.

Ones Density: the measure of the number of logical 1s on a T1 line compared to a given total number of bits on that line; used for timing information in data recovery in AMI and B8ZS.

On-Hook: The condition of a device which has not accessed a phone line. In modem use, this is equivalent to a telephone handset that has not been picked up. In other words, it can receive an incoming call. Contrast "off-hook".

Open Shortest Path First (OSPF): A hierarchical Interior Gateway Protocol (IGP) routing algorithm for IP that is a proposed standard for the Internet. OSPF incorporates least-cost routing, equal-cost routing, and load balancing.

Outage: The measure of the time during which a circuit is not available for use due to service interrupt. Outage is the complement of circuit "availability" (100% minus % available = % outage).

Out-of-band: Signaling that is separated from the channel carrying the information (e.g., the voice/data/video signal is separate from the carrier signal). Dialing and various other "supervisory" signals are included in the signaling element. Contrast "In-band" signaling.

Out of Frame (OOF): A T1 alarm condition that is logged on the loss of 2, 3 or 4 of 5 consecutive FT framing bits.

P

Packet: 1. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals and, possibly, error control information are arranged in a specific format. 2. Synonymous with data frame. 3. In TCP/IP, the unit of data passed across the interface between the Internet layer and the link layer. A packet includes an IP header and data. A packet can be a complete IP datagram or a fragment of an IP diagram. 4. In X.25, a data transmission information unit. A group of data and control characters, transferred as a unit, determined by the process of transmission. Commonly used data field lengths in packets are 128 or 256 bytes. 5. The field structure and format defined in the CCITT X.25 recommendation.

Packet Assembler/Dissembler (PAD): Used by devices to communicate over X.25 networks by building or stripping X.25 information on or from a packet.

Packet Data: The information format ("packetized") used for packet-mode calls.

Packet Mode: Refers to the switching of chunks of information for different users using statistical multiplexing to send them over the same transmission facility.

Parity bit: An extra bit attached to each byte of synchronous data used to detect errors in transmission.

Permanent Virtual Circuit (PVC): A connection between two endpoints dedicated to a single user. In ISDN, PVCs are establised by network administration and are held for as long as the user subscribes to the service.

Physical Unit (PU): The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only.

Point of Presence (POP): The central office's end points of the long distance carriers.

Point-to-Point Protocol (PPP): A protocol that lets a PC user access TCP/IP (Internet memeber) using an ISDN terminal adapter or a high-speed modem over a standard telephone line.

Port: A location for input or output data exchange. Computers, muxes, etc. have ports for various purposes.

Primary Rate Interface (PRI): Used on ISDN. In North America, and Japan, PRI is one 64Kbps D channel and 23 B channels. Elsewhere, it is one D channel and 30 B channels.

Primitive: An abstract representation of interaction across the access points indicating that information is being passed between the service user and the service provider. The OSI Reference Model defines four types of primitives: Request, Indication, Response and Confirm.

Private Branch Exchange (PBX): A telephone exchange located on the customer's premises. The PBX provides a circuit switching facility for telephone extension lines within the building, and access to the public telephone network. See also "Exchange".

PROM (Programmable Read Only Memory - pronounced "prom"): A permanent memory chip that can be programmed or filled by the customer after by the manufacturer has set initial values. Contrast with ROM.

Protocol: 1. A set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. 2. In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. 3. In SNA, the meanings of and the sequencing rules for requests and responses used for managing the network, transferring data, and synchronizing the states of network components. 4. Synonomous with line control discipline.

Proxy Server: A secure gateway that provides multiple LAN users with high performance Internet access by functioning as a TCP/IP proxy server that resides on the outer edge of a firewall.

PSTN (Public Switched Telephone Network): A worldwide public voice telephone network that is used as a telecommunications medium for the transmission of voice, data and other information.

Public Data Network (PDN): A packet-switched network that is available to the public for individual ("subscriber") use. Typically, controlled by a government or a national monopoly.

Public Switched Telephone Network (PSTN): The group of circuit-switching voice carriers, which are commonly used as analog data communications services.

Pulse Code Modulation (PCM): 1. In data communication, variation of a digital signal to represent information; for example, by means of pulse amplitude modulation (PAM), pulse duration modulation (PDM), or pulse position modulation (PPM). 2. Transmissions of analog information in digital form through sampling and encoding the samples with a fixed number of bits.

Pulse dialing: One of two methods of dialing a telephone, usually associated with rotary-dial phones. Compare with "tone dialing".

Q

Quantizing: The process of analog-to-digital conversion by assigning a range, from the contiguous analog values, to a discrete number.

R

Random Access Memory (RAM): A computer's primary workspace. All data must be stored in RAM (even for a short while), before software can use the processor to manipulate the data. Before a PC can do anything useful it must move programs from disk to RAM. When you turn it off, all information in RAM is lost.

Rate Enforcement: The concept in frame relay where frames sent faster than the CIR are to be carried only if the bandwidth is available, otherwise they are to be discarded. (The frame relay network assumes that anything exceeding the CIR is of low priority.) Rate enforcement makes sure that the network will not get so congested that it isn't able to meet the agreed on CIR.

Recognized Private Operating Agency (RPOA): A corporation, private or government-controlled, that provides telecommunications services. RPOAs, such as AT&T, participate as non-voting members in the CCITT.

Red Alarm: A T1 error condition generated when a local failure (e.g., loss of synchronization) exists for 2.5 seconds, causing a Carrier Group Alarm (CGA). See also "Blue Alarm" and "Yellow Alarm".

Request for Comment (RFC): A set of papers in which Internet standards (published and proposed), along with generally-accepted ideas, proposals, research results, etc. are published.

Ring Down Box: A device that emulates a CO by generating POTS calls for testing and product demos.

Ring Down Circuit: A tie line connecting phones where picking up one phone automatically rings another phone. A feature used for emergencies to alert the person at the other phone of the incoming call.

RJ-11: An industry standard interface used for connecting a telephone to a modular wall outlet; comes in 4-and 6-wire packages.

RJ-45: An 8-wire modular connector for voice and data circuits.

Robbed Bit Signaling: The popular T1 signaling mechanism where the A and B bits are sent by each side of the T1 termination and are "buried" in the voice data of each voice channel in the T1 circuit. Since the bits are "robbed" infrequently, voice quality remains relatively uncompromised. See "bit robbing". The robbed-bit signaling technique is used in D4 channel banks to convey signaling information. The eighth (least significant) bit of each of the 24 8-bit time slots is "robbed" every sixth frame to convey voice-related signaling information such as on-hook, off-hook, etc, for each channel.

Router: A device that connects two networks using the same networking protocol. It operates at the Network Layer (Layer 3) of the OSI model for forwarding decisions.

Routing Information Protocol (RIP): A distance vector-based protocol that provides a measure of distance, or hops, from a transmitting workstation to a receiving workstation.

RS232-C: An EIA standard for a serial interface between computers and peripheral devices (modem, mouse, etc.). It uses a 25-pin DB-25, or a 9-pin DB-9 connector. The RS-232 standard defines the purposes, electrical characteristics and timing of the signals for each of the 25 lines.

RS-422: The EIA standard for a balanced interface with no accompanying physical connector. RS-422 products can use screw terminals, DB9, various DB25, and DB37 connectors.

RS-530: The EIA standard for the mechanical/electrical interface between DCEs and DTEs transmitting synchronous or asynchronous serial binary data. RS-530 provides for high data rates with the same connector used for RS-232; however, it is incompatible with RS-232.

S

Serial Port: The connector on a PC used to attach serial devices (those that need to receive data one bit after another), such as a mouse, a printer or a modem. This consists of a 9- or 25-pin connector that sends data in sequence (bit by bit). Serial ports are referred to as “COMx” ports, where x is 1 to 4 (i.e., COM1 through COM4). A serial port contains a conversion chip called a “UART” which translates between internal parallel and external serial formats.

Service: The requirements offered by an RPOA to its customers to satisfy specific telecommunications needs.

Severely Errored Seconds (SES): Refers to a typical T1 error event where an error burst occurs (a short term, high bit-error rate that is self-clearing). Per the ITU-T (CCITT) G.821: any second in which the BER is less than 1x10 -3 .

Signaling: The process of establishing, maintaining, accounting for, and terminating a connection between two endpoints (e.g., the user premises and the telco CO). Central office signals to the user premises can include ringing, dial tone, speech signals, etc. Signals from the user’s telephone can include off-hook, dialing, speech to far-end party, and on-hook signals. In-band signaling techniques include pulse and tone dialing. With common channel signaling, information is carried out-of-band.

Simple Network Management Protocol (SNMP): TCP/IP protocol that allows network management.

Simultaneous Voice Data (SVD): A technology for letting a user send data via a modem, and use a handset to talk to another user at the same time over the same connection. The alternative, making a second call, can be expensive or even impossible. The uses for SVD are telecommuting, videoconferencing, distant learning, tech support, etc.

Stop Bit: One of the variables used for timing in asynchronous data transmission. Depending on the devices, each character may be trailed by 1, 1.5, or 2 stop bits.

Superframe (D4): A T1 transmission fromat that consists of 12 DS1 frames, or 2316 bits. A DS1 frame consists of 193 bit positions. A frame overhead bit is in the first position, and it is used for frame and signaling phase alignment only.

Subscriber Loop: See “Local loop”.

Switched 56: A circuit-switched (full duplex digital synchronous data transmission) service that lets you dial a number and transmit data to it at 56K bps. It is a relatively low cost service, widely used in North America for telecommuting, videoconferencing and high speed data transfers. Many phone companies are (or will be) phasing out Switched 56 in favor of ISDN service.

Switched Virtual Circuit (SVC): A type of data transmission where the connection is maintained only until the call is cleared.

Switched Line: In communications, a physical channel established by dynamically connecting one or more discrete segments. This connection lasts for the duration of the call after which each segment can be used as part of a different channel. Contrast with leased line.

Switched Network: A network in which a temporary connection is established from one point via one or more segments.

Synchronous Data Link Control (SDLC): A discipline conforming to subsets of the Advanced Data Communications Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex, or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop.

Synchronous Transmission: The transmission of data which involves sending a group of characters in a packet. This is a common method of transmission between computers on a network or between modems. One or more synchronous characters are transmitted to confirm clocking before each packet of data is transmitted. Compare to Asynchronous Transmission.

Systems Network Architecture (SNA): The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of networks.

T

Tariff: The rate/availability schedule for telephone and ISDN services from a regulated service provider.

TCP/IP: A set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks.

T Carrier: The generic name for a digitally multiplexed carrier system. In the North American digital hierarchy, a T is used to designate a DS (digital signal) level hierarchy. Examples: T1 (DS1) is a 1.544 M bps 24-channel designation. In Europe, T1 is called E1. The T Carrier system was originally designed for transmitting digitized voice signals, but has since been adapted for digital data applications.

T1: A digital transmission link capable of 1.544M bps. T1 uses two pairs of normal UTP, and can handle 24 voice conversations, each digitized at 64K bps. T1 is a standard for digital transmission in the U.S., Canada, Japan and Hong Kong. T1 is the access method for high-speed services such as ATM, frame relay, and SMDS. See also T Carrier, T1 line and FT1.

T1 Channel Tests: A set of diagnostics that vary by carrier, used to verify a T1 channel operation. Can include Tone, Noise Level, Impulse Noise Level, Echo Cancelers, Gain, and Crosstalk testing.

T1 Framing: To digitize and encode analog voice signals requires 8000 samples per second (twice the highest voice frequency of 4000 Hz). Encoding in an 8-bit word provides the basic T1 block of 64K bps for voice transmission. This “Level 0 Signal, as its called, is represented by “DS-0”, or Digital Signal at Level 0. 24 of these voice channels are combined into a serial bit stream (using TDM), on a frame-by-frame basis. A frame is a sample of all 24 channels; so adding in a framing bit gives a block of 193 bits (24x8+1=193). Frames are transmitted at 8000 per second (the required sample rate), creating a 1.544M (8000x193=1.544M) transmission rate.

T1 Line: A digital communications facility that functions as a 24-channel pathway for data or voice transmission. A T1 line is composed of two separate elements: the Access element and the Long Haul element.

T1 Mux: A device used to carry many sources of data on a T1 line. The T1 mux assigns each data source to distinct DS0 time slots within the T1 signal. Wide bandwidth signals take more than one time slot. Normal voice traffic or 56/64K bps data channels take one time slot. The T1 mux may use an internal or external T1 DSU; a “channel bank” device typically uses an external T1 CSU.

Transmission Control Protocol / Internet Program (TCP/IP): A multi-layer set of protocols developed by the US Department of Defense to link dissimilar computers across dissimilar and unreliable LANs.

Terminal: The screen and keyboard device used in a mainframe environment for interactive data entry. Terminals have no “box”, which is to say they have no file storage or processing capabilities.

Terminal Adapter (TA): An ISDN DTE device for connecting a non-ISDN terminal device to the ISDN network. Similar to a protocol converter or an interface converter, a TA connects a non-ISDN device between the R and S interfaces. Typically a PC card.

Tie line: A dedicated circuit linking two points without having to dial a phone number (i.e., the line may be accessed by lifting the telephone handset or by pushing a button).

Time-Division Multiplexing (TDM): Division of a transmission facility into two or more channels by allotting the common channel to several different information channels, one at a time.

Time Slot: One of 24 channels within a T1 line. Each channel has a 64K bps maximum bandwidth. “Time slot” implies the time division multiplexing organization of the T1 signal.

Toll Call: A call to a location outside of your local service area (i.e., a long distance call).

Tone dialing: One of two methods of dialing a telephone, usually associated with Touch-Tone® (push button) phones. Compare with pulse dialing.

Topology: Physical layout of network components (cables, stations, gateways, and hubs). Three basic interconnection topologies are star, ring, and bus networks.

Transmission Control Protocol (TCP): A communications protocol used in Internet and in any network that follows the US Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It assumes that the Internet protocol is the underlying protocol.

Transport Layer: Layer 4 of the Open Systems Interconnection (OSI) model; provides reliable, end-to-end delivery of data, and detects transmission sequential errors.

Transport Protocol Data Unit (TPDU): A transport header, which is added to every message, contains destination and source addressing information that allows the end-to-end routing of messages in multi-layer NAC networks of high complexity. They are automatically added to messages as they enter the network and can be stripped off before being passed to the host or another device that does not support TPDU's.

Trunk: Transmission links that interconnect switching offices.

TSR (terminate and stay resident): A software program that remains active and in memory after its user interface is closed. Similar to a daemon in UNIX environments.

Tunneling: Encapsulation data in an IP packet for transport across the Internet.

Twisted pair wiring: A type of cabling with one or more pairs of insulated wires wrapped around each other. An inexpensive wiring method used for LAN and telephone applications, also called UTP wiring.

U

UART (Universal Asynchronous Receiver/Transmitter) (pronounced "you art"): A chip that transmits and receives data on the serial port. It converts bytes into serial bits for transmission, and vice versa, and generates and strips the start and stop bits appended to each character.

UNIX: An operating system developed by Bell Laboratories that features multiprogramming in a muti-user environment.

Unshielded Twisted Pair (UTP): Telephone-type wiring. Tansmission media for 10Base-T.

V

V.25bis: An ITU-T standard for synchronous communications between a mainframe or host and a modem using HDLC or other character-oriented protocol.

V.54: The ITU-T standard for local and remote loopback tests in modems, DCEs and DTEs. The four basic tests are:

- local digital loopback (tests DTE send and receive circuits),
- local analog loopback (tests local modem operation),
- remote analog loopback (tests comm link to the remote modem), and
- remote digital loopback (tests remote modem operation).

Virtual Circuit: A logical connection. Used in packet switching wherin a logical connection is established between two devices at the start of transmission. All information packets follow the same route and arrive in sequence (but do not necessarily carry a complete address).

W

Wide Area Network (WAN): 1. A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. 2. A data communications network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. Contrast with local area network (LAN).

Wide Area Telecommunications Service (WATS): A low-cost toll service offered by most long distance and local phone companies. Incoming (800 call service, or IN-WATS) and outgoing WATS are subscribed to separately, but over the same line.

X

X.25: ITU-T's definition of a three-level packet-switching protocol to be used between packet-mode DTEs and network DCEs. X.25 corresponds with layer 3 of the 7-layer OSI model.

Y

Yellow Alarm: An error indication sent by the T1 device when it has not gotten a receive signal, or cannot synchronize on the receive signal received. Contrast "Red Alarm" and "Blue Alarm".

Z

Zero Byte Time Slot Interchange (ZBTSI): A method for allowing 64K bps unrestricted user data (allowing all 0s in the user data). An alternative to (but not as popular as) B8ZS.

Index

A

About the Internet 56
About the Multi-Tech Fax-Back Service 56
Adding Proxy Applications 36
Applications 42
Archie 59

B

Back Panel 9
  Connectors 9
BBS 55

C

Cabinet Mounting Screw 13
Cabling Your ProxyServer 14
Changing IP Parameters 33
Changing WAN Port Parameters 35
Command Connector 9
Configuration Port Setup 31
Connectors 9
  10Base-T 9
  Command 9
  Ethernet 1 and 2 9
  Power 9
  RS232/V.35 9

D

Data Communications Equipment 9
DCE. *See* Data Communications Equipment
DHCP Client 33
DHCP Relay Agent 34
DHCP Server 38
DNS 59
Download Firmware Update 31

E

Enabling the DHCP Server 38
Ethernet 1 and 2 Connectors 9

F

Fax-Back Service 56
Filtering 40
Finger 59
Firewall Configuration 32
Firewall Program Group 30
Firewall Software 26
Front Panel 8
  LEDs 8
FTP 59

G

Gopher 59

H

HTML 59
HTTP 59

I

Internet 56
Internet Gateway Parameters 34
Internet LAN Port Parameters 33
Internet Protocol 58, 60
Internet Services Network 6
IP 60
IP Parameters 33

L

LEDs 8
  ETHERNET 1 and 2 8
  Fail 8
  Power 8
  WAN Link 8
Limited Warranty 52
Loading Your Software 18

O

On-line Warranty Registration 52

P

Ping 59
POP 59
Power Connector 9
Program Group 30
Proxy Applications 36

R

Remote Configuration
  LAN-Based Procedure 46
Remote Management 48
  Telnet 48
  WEB Management 50
RS232/V.35 Connector 9

S

Safety Warnings 12
Secured LAN Port Parameters 33
Service 54
Shunt Positions 13
SMTP 59
SNMP 59

Software 26
Applications 42
Configuration Port Setup 31
DHCP Server 38
Download Firmware Update 31
Filtering 40
Firewall Configuration 32
IP Parameters 33
Loading 18
Program Group 30
Proxy Applications 36
Statistics 42
Uninstall Firewall Configuration 31
WAN Port Parameters 35
Specifications 10
Statistics 42

T

TCP/IP 58
Tech Support 53
Technical Specifications 10
Telnet 48, 59
The Multi-Tech BBS 55
Traceroute 59
Transmission Control Protoco 58
Typical Applications 26
Configuration 1 - Cable/DSL Modem 26
Configuration 2 - Existing Dual-LAN with Router 27
Configuration 3 - New Dual-LAN with T1 DSU 28

U

Uninstall Firewall Configuration 31
Unpacking Your ProxyServer 12

V

V.35 Shunt 13
V.35 Shunt Procedure 13
Virtual Servers
Enabling 41

W

WAN Port Parameters 34, 35
Warranty 52
On-line Warranty Registration 52
WEB Management 50
Whois/NICNAME 59